China's Digital Power

Assessing the Implications for the EU

January 2022

Editor: Tim Rühlig

About the Digital Power China research consortium

The Digital Power China research (DPC) consortium is a gathering of China experts and engineers based in eight European research institutions, including universities and think tanks. In addition, a European non-resident fellow of a US research institution has joined DPC. The group is devoted to track and analyse China's growing footprint in digital technologies and its implications for the European Union. Based on interdisciplinary research DPC offers concrete policy advise to the EU. Tim Rühlig, Research Fellow at the German Council on Foreign Relations (DGAP), is the convenor of DPC and co-chairs the initiative with Carlo Fischione, who is a Professor at the Royal Institute of Technology in Stockholm.

DPC systematically pairs technological and country expertise. It is based on rigorous academic research that is combined with experience in the provision of policy advice. The informal group brings together a variety of European researchers in order to pair diverging perspectives from across the continent. Responsibility relies solely with the indicated authors of the chapters and papers published by DPC.[1]

At the time of writing the chapters, the participating researchers were affiliated with the following institutions:

- Belgium: KU Leuven
- France: French Institute of International Relations (IFRI), Paris
- Germany: German Council on Foreign Relations (DGAP), Berlin
  Jacobs University Bremen
  Mercator Institute for China Studies (MERICS), Berlin
  Stiftung Neue Verantwortung (SNV), Berlin
- Greece: Athens University of Economics and Business
- Italy: University of Insubria, Varese/Como
  University of L'Aquila
- Latvia: Riga Stradins University
- The Netherlands: Clingendael Institute, The Hague
  Leiden Asia Centre at Leiden University
- Sweden: The Royal Institute of Technology (KTH), Stockholm
  The Swedish Institute of International Affairs (UI), Stockholm
  Uppsala University (UU)
- United States Belfer Center for Science and International Affairs, Harvard University, Cambridge

[1] The production of this report has been supported through the COST Action CA18215 - China In Europe Research Network (CHERN - www.china-in-europe.net), supported by the European Cooperation in Science and Technology (COST - www.cost.eu).


DPC

Table of content


DPC

Getting China's digital technology policy right: implications for the EU

Rogier Creemers, Carlo Fischione, Tim Rühlig

Abstract

The rapid emergence of China as a technical power creates a spectrum of new challenges for Europe to engage with, covering the economic, political, security and ideational fields. Meeting these challenges will require, first and foremost, gaining greater knowledge of China's digital ambitions and their impact on Europe. To make sense of China digital technology ambitions, it is necessary to question long-held beliefs on how digital economies develop and how state and technologies interact, and to take China's ambitions seriously, even if we critically assess their relevance and feasibility. This introductory chapter outlines a framework for such analysis and carves out how the Digital Power China consortium could contribution to the process of recalibrating EU policy in light of China's growing technological footprint.

Digital technologies and connectivity alongside a new industrial revolution are driving societal transformation. To stay abreast of these developments the European Union (EU) has drawn up its "Fit for the Digital Age" agenda, which will have to be implemented to maintain any chance of a prosperous future for the citizens of its member states.[2] Alongside the intra-European dimension, the EU's digital ambitions are influenced by external conditions. Technological progress is not just a matter of economic competitiveness, it is at the core of the emerging power rivalry between the United States (US) and the People's Republic of China (PRC). At a time when, broadly speaking, the EU relies on US software and East Asian hardware, including from China, the exploitation of technological dependencies for the purposes of power politics could constrain the EU's ability to act with full sovereignty and autonomy. It is against this backdrop that the EU is debating "technological sovereignty" for the sake of

[2] European Commission, "A Europe Fit for the Digital Age", *EU*, accessed 6 August 2021, at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en.

"open strategic autonomy".[3] Since digital technologies now penetrate all areas of society, cybersecurity is of pivotal importance. Sabotage, espionage and intrusion into digital infrastructure and basic applications could disrupt the functioning of Europe. To malign actors, increasingly interconnected economies make cyberespionage more attractive than ever before.

The EU needs to learn quickly how to navigate these relatively new waters. Central to this process will be to properly understand, and adopt a strategy on, China. China's footprint in digital technologies is heavy and rapidly evolving. Unlike the US, the PRC is not a security ally of the EU or its member states. Moreover, the development of and the policies that structure the digital technology ecosystems of the EU and China are shaped by fundamentally different economic and political systems.

China's presence in digital technology overlaps with European priorities, interests and concerns in myriad ways. China's growing role in 5G telecommunications has raised questions across the continent about supply chain security and possible espionage.[4] Both state-sponsored economic espionage and influencing operations have gained equal priority on the European policy agenda.[5] The growing domestic use of surveillance technologies, particularly in Xinjiang, puts China at odds with European views of fundamental values.[6] The Digital Silk Road, China's ambitious project to expand connectivity and digital technology across the Global South, intersects with the EU's global development strategy. China's stated ambitions for leadership in areas such as Artificial Intelligence (AI) and big data have thrown into sharp relief the question of not only how Europe should regulate these at home, but also how Chinese approaches might affect the emergence of a global, data-fuelled economic and political structure. The growing presence of Chinese actors in technical standardisation bodies has led to concerns that China might set the rules for future technological development paths in order to anchor its political model in technical norms.[7] China's high barriers to market access and high levels of state aid to its digital companies have tilted the playing field against

[3] European Political Strategy Centre, *Rethinking Strategic Autonomy in the Digital Age*, Brussels, European Commission, 2019.
[4] Tim Rühlig and Maja Björk, "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe", *UI Paper 1/2020*, Stockholm, The Swedish Institute of International Affairs, 2020.
[5] Mark Scott et al., "European Commission Accuses China of Peddling Disinformation", *Politico*, accessed 24 October 2021, at https://www.politico.eu/article/european-commission-disinformation-china-coronavirus/.
[6] European Parliament, "Forced Labour and the Situation of the Uyghurs in the Xinjiang Uyghur Autonomous Region", *European Parliament*, accessed 24 October 2021, at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0375_EN.html.
[7] Tim Rühlig, *Technical Standardisation, China and the Future International Order. A European Perspective*, Brussels, EU Office of the Heinrich Böll Foundation, 2020; John Seaman, *China and the New Geopolitics of Technical Standardization. Notes de l'Ifri*, Paris, Ifri, 2020.

European companies both inside Chinese markets and globally.[8]

Notwithstanding all these well-founded concerns, technological decoupling and ceasing all cooperation with the PRC on digital technologies is neither desirable nor feasible. Even without considering the spillover effects that such a move might have on other areas of European-Chinese relations, there would be severe impacts on: the welfare of European consumers; the ability of European businesses to operate in Europe, in China and elsewhere; the ability of European knowledge generators and research institutions to attract innovative talent or perform cutting-edge research; and the security of the European continent.

European consumers and infrastructure vendors rely on Chinese manufacturing capabilities for the vast majority of the digital devices they purchase. Moving these production chains out of China would require vast amounts of time and resources. Technology has also been integrated into traditional products such as cars, for which China is still one of the world's largest – and fastest-growing – markets, and where Europe has a strong position. It is also worth reflecting on the changed perception of mutual interdependence. Not long ago, this was held to be a source of security and stability; now it is primarily seen as a risk and a threat. It is, of course, both, but the destabilising effects of further decoupling, as fewer stakeholders stand to gain from at least cordial relations, are important to keep in mind. Furthermore, one of the key bottlenecks in digital development is the scarcity of talent. Europe and China have both profited considerably from collaboration on research and development in universities and corporations. This could be put at risk in case of severe decoupling.

In a nutshell, China remains a complex actor for EU policymaking, and for this reason the EU's "Strategic Outlook" on China characterises the PRC concurrently as a "partner", "competitor" and "systemic rival".[9] The general discussion on what China's multiple roles mean for the EU's China policy writ large is significantly shaped by how that question is being answered in the field of digital technologies.

One example of how the intersection of the omnipresence of digital technologies and China's multiple roles affects the EU's agenda is combating climate change. Climate change is often cited as an exemplary area in which the EU needs to cooperate with China, not least because the PRC is the largest contributor to the emission of greenhouse gases. Unless China massively reduces its emissions, combating climate change is doomed to fail. New technologies will be key to achieving carbon neutrality.

[8] BusinessEurope, *The EU and China. Addressing the Systemic Challenge. A Comprehensive EU Strategy to Rebalance the Relationship with China*, Brussels, BusinessEurope, 2020.

[9] European Commission, *EU-China: A Strategic Outlook. European Commission and HR/VP Contribution to the European Council. 12 March 2019*, Brussels, European Commission, 2019.

Digitalisation is expected to have a major role in attempts to reduce emissions. One of the most prominent examples is the digitalisation of the production and distribution of electrical power in grids, moving towards the realisation of the smart grids. In such grids, the integrated distribution of renewable energy generation and its coordination through the Internet and new wireless communications standards, such as 5G, will significantly reduce the cost of the production and distribution of energy, and significantly reduce greenhouse gas emissions. In the next decade, it is likely that the evolution of Internet services will introduce extended and augmented reality services, so that people in distant locations will be able to interact over the Internet as if they were in the same room. Clearly, this will reduce the need for private and public transportation. Similarly, the introduction of autonomous vehicles capable of coordinating their speed and direction according to the traffic will significantly reduce energy use.

However, as these technological predictions are made, it is also clear that the overall digitalisation of systems and society will result in increased demands for energy production. While it is likely that greenhouse gas emissions will be reduced in the locations where energy is used (e.g., in urban environments), there is a risk that the production sites for energy could still contribute to major negative emissions, especially where the costs of replacement with or the installation of green energy production are very high compared to traditional methods.

Notwithstanding the EU's interest in China developing and using new digital technologies for these purposes, the PRC is also a competitor of European industry in this field. Between 1990 and 2014, the number of environment-related patents in China increased by more than 60 times.[10] China's efforts are heavily subsidised by the party-state. For example, in 2013, 14.8 percent of national high-tech R&D funding was already being allocated to green tech innovation.[11] China's research efficiency might still be remarkably low, but it would be unwise to work on the assumption that Chinese engineers will not come up with competitive technological solutions.[12] This EU-China competition over green digital technology is distinct because of the persistent lack of a level playing field and the high level of state support, which are part of the systemic rivalry between the two entities.[13]

[10] OECD, "China's Progress towards Green Growth. An International Perspective", *OECD*, accessed 2021-10-24, at https://www.oecd.org/env/country-reviews/PR-China-Green-Growth-Progress-Report-2018.pdf.

[11] Ministry of Science and Technology of the People's Republic of China, "国家科技计划年度报告 2013", *MOST*, accessed 24 October 2021, at http://www.most.gov.cn/xxgk/xinxifenlei/fdzdgknr/zfwzndbb/201404/t20140422_112822.html.

[12] Anna Holzmann and Nis Grünberg, ""Greening" China: An Analysis of Beijing's Sustainable Development Strategies", *Merics*, accessed 2021-10-24, at https://merics.org/sites/default/files/2021-03/MERICSChinaMonitor%20GreeningChina%202.pdf.

[13] Janka Oertel et al., "Climate Superpowers: How the EU and China Can Compete and Cooperate for a Green Future", *ECFR*, accessed 2021-08-06, at https://ecfr.eu/wp-content/uploads/Climate-superpowers-How-the-EU-and-China-can-compete-and-cooperate-for-a-green-future.pdf.

The four-dimensional "digital China challenge"

China might be a complex actor with multiple roles, but it is the systemic rivalry that requires most attention. This is not because systemic rivalry should predominate the other roles, but because the coexistence of partnership and competition is common practice in foreign policymaking while systemic rivalry is not. In the field of digital technologies, the Digital Power China (DPC) research consortium has identified a *four-dimensional* "China challenge" for the EU with overlapping economic, political, security and ideational features:

- *Economically*, a tilted playing field favours Chinese tech firms that benefit from preferential treatment and lower data protection and environmental standards. This endangers the EU's digital industrial competitiveness. In addition, technological decoupling has enormous potential for economic fall-out for the EU.
- *Politically*, China can leverage political concessions from technologically (over-)dependent third countries, including EU member states. The PRC is also actively engaging with global cyber-governance in an effort to rewrite institutional processes and increase its power.
- In the *security field*, China presents multiple concerns, ranging from Chinese espionage to technical hacking and social media-based influencing operations, and the security concerns that result from China-based hardware vendors or manufacturing chains. These concerns are not mitigated by a common security understanding or formal cooperation with Beijing. Furthermore, the incorporation of Chinese digital equipment could be accompanied by cyber-insecurities that enable espionage and sabotage by a state with which the EU has no security alliance.
- *Ideationally*, China's technological stronghold calls into question whether the governance principles of the digital technologies that are increasingly penetrating entire societies reflect liberal and democratic values. Among the notably divergent fields of ideational conception between Europe and China are technical standards, data governance and effective protection of the environment.

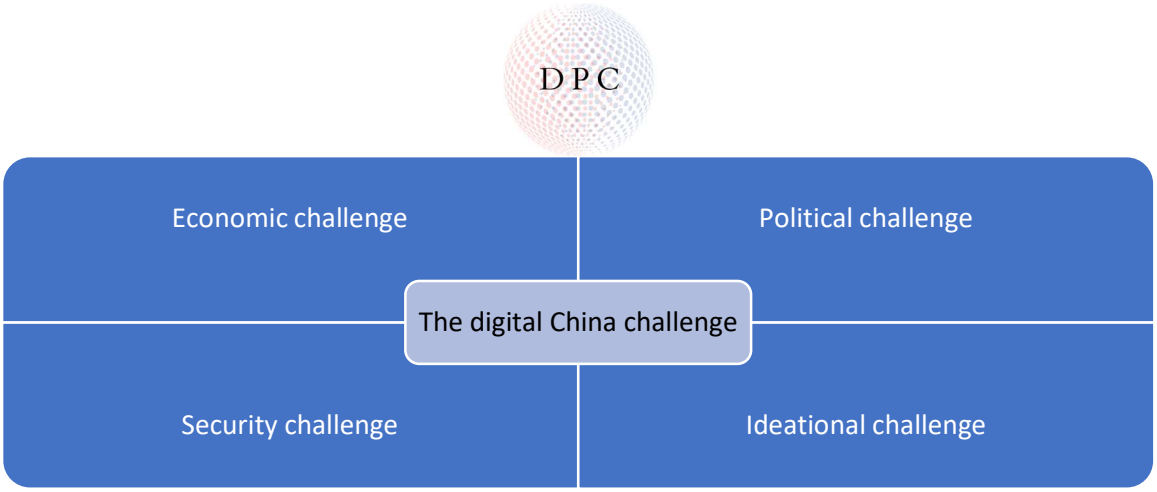

Figure 1: The four-dimensional digital China challenge. Source: Own graphic.

The EU member states cannot be expected to address these challenges alone: a unitary EU approach is essential. Even then, the EU will need to cooperate closely with like-minded partners if it is to meet the four-dimensional China challenge. While transatlantic cooperation is growing stronger once again under the Biden administration, EU interests and strategies are still not entirely congruent with those of the US. Consequently, the EU rightly continues to discuss its own "open strategic autonomy", which requires independent European knowledge of China's digital ambitions and the development of a well-grounded EU position on these developments.

Questioning long-held beliefs

The unfolding of digital technologies and the growth of China's global footprint are intertwined, and each has been rapid and transformative. Hence, an independent EU position must begin with a questioning of long-held beliefs and an assessment of the intersection of China's increasing influence and the global digital transformation.

Key enabling technologies such as AI, the Internet of Things (IoT) or 5G are only umbrella terms from which a highly complex and diverse set of use cases and applications emerges. The IoT refers to a large group of communications technologies that will be used to connect physical objects, systems or large-scale infrastructure via communication networks. Once the IoT can provide data about these objects, systems or infrastructure, it will provide tremendous monitoring opportunities. The data collected will be used by AI algorithms to identify or understand phenomena and trends in human behaviour, while at the same time automatically enforcing decisions or regulations without any human intervention. While these technologies are already taking shape, they will have complex and transformative effects on society in the next two decades. One facilitator of such a transformation is the development of the Internet and the introduction of 5G, which is a first attempt at a communication standard for "cellular wireless networks" that offers a

unified approach to the connectivity of many existing IoT standards. Thanks to 5G, implementation of the IoT and AI will be able to make a leap forward, with major effects on all aspects of societal (civilian and military) and technological transformation processes. Among these can be mentioned blockchain, digital green transformation and supply chain security. All this is triggering a plethora of fundamental questions that must be carefully addressed. These are briefly outlined below.

To control or monitor such a tremendous transformation, it will be essential to define technical standards for the IoT and AI in cooperation with the world's major player. Given that these technologies will radically change society, they will have to be open and implementable by many different players. The imposition of closed standards or mutually competing standards is likely to have difficult-to-imagine consequences.

The definition of shared standards will be essential for cybersecurity. As the complexity of technological systems increases and society becomes increasingly reliant on these systems, major technical and political coordination efforts will be needed in the coming years and decades to embed in shared technical standards the means to monitor the behaviour of the technological systems or block attempts to attack or even destroy them.

While the benefits and risks of the above-mentioned transformation are often associated with software components, an additional technological aspect is the hardware component and therefore the role of semiconductors. For those who are unable to control the production of electronic components, there will be inherent risks of scarcity and high prices in the development of IoT- and AI-related systems, as well as the potential for cyberattack and threats to be embedded in the architectures of these electronic components.

The technological transformation is not the only megatrend that the EU will have to properly understand. China's emergence as a technology power presents the EU with a reality it did not expect. For decades, Europeans ascribed Western digital prowess to the beneficial combination of liberal democracy and free market capitalism. This combination alone provided the environment for inquiry, openness and enterprise deemed necessary for technological success. Obviously, as a non-democratic, non-free-market state, China would be unable to emulate this success. As recently as 2014, journals such as the *Harvard Business Review* could get away with publishing articles on "Why China Can't Innovate".[14]

This view turned out to have been misguided. Not only do Chinese capabilities now rival those of the EU and the US, but we have also underestimated the

[14] Regina M. Abrami et al., "Why China Can't Innovate", *Harvard Business Review*, accessed 18 September 2021, at https://hbr.org/2014/03/why-china-cant-innovate.

skills base that China has rapidly developed as a manufacturer of electronic goods designed or developed elsewhere. For at least the past decade, China has been an integral and irreplaceable part of the global digital ecosystem with considerable competitive advantages of its own. We therefore need to develop ideas and concepts that can account for China's competence in the field of technology and, more broadly, for its growing global footprint. This may be difficult, as it removes the centrality of a western narrative that lies at the core of the self-perceptions of states and societies. However, as China has already profoundly reshaped the global digital order, the less time spent on coming to terms with the consequences, the better.

Europeans tend to discuss the role of US corporations in a critical way, but China is not a monolithic actor either. The public-private divide merits attention. While there is a considerable degree of proximity between Chinese corporations and the party-state, the recent regulatory wave targeting the digital sector demonstrates that it is incorrect to see Chinese corporations as a mere manifestation of Chinese Communist Party (CCP) interests. This means that some of the multiple players in China will be closer to European interests than others, even if none will ever fully align. Even within government, security bodies have different interests to the military, or to the technological bureaucracy. A policy aimed at achieving European objectives should be cognisant of the fact that modes of cooperation can be found with some Chinese actors, but not with others.

Filling the knowledge gap

Making sense of China's digital technology ambitions implies a need to *understand* the PRC's approach as much as possible through a Chinese lens. Explanation does not equate to justification. Just because a researcher displays the cognitive empathy needed to make sense of what is happening in China does not mean that they approve of it. The EU should neither be naive about China's ambitions and the role of digital technological advances, nor label everything dangerous just because it comes from China.

Often, Chinese policy decisions are explained with simple reference to the CCP's putative desire to exert control; but just because China is an authoritarian state does not mean that everything it does contains authoritarian elements. Regime type matters but does not explain everything. It is important to carefully consider whether a given policy is furthering authoritarianism. If this is the premise from the start, however, it can often obscure as much as illuminate. For instance, China's attempts to expand the global footprint of its technology companies might be intended to assist with

the global implementation of CCP ideology, but it can certainly also be explained by the simple expedient of money. China is seeking new sources of economic growth and export income.[15] Independent analysis is necessary to investigate specific cases before conclusions can be drawn.

Similarly, the Chinese Social Credit System is often presented as an "Orwellian" effort to use digital technology to achieve comprehensive control over the individual, including by senior politicians.[16] The far-reaching potential of the Social Credit System is beyond doubt. This potential has hardly been used, however, and currently the system is mostly deployed to enhance regulatory compliance in certain specific areas.[17] Thus, analyses must neither be blind to the potential of a system nor distort how it is being used at present.

The secrecy of China's Leninist system is often blamed for our lack of understanding,[18] and there is some justification for this. The Chinese government is less transparent than the EU, and its efforts to manage the availability of information are well known. Recent moves by the Chinese government, including placing sanctions on European researchers, research institutes and parliamentarians, further complicate a proper understanding. This is important because China has many distinctive characteristics. At the same time, however, the EU needs to understand that the PRC also shares many policy objectives and interests with countries worldwide and displays similar trends. China's emerging personal information protection regime, anti-monopoly regime for online platforms and online consumer protection regulations, while not congruent, bear similarities to the General Data Protection Legislation, and the EU Digital Markets and Digital Services Acts currently in the legislative pipeline.[19] To derive the best available analysis, it is necessary to engage with the country in all its complexities and nuances.

For example, China has recently adopted its 14th Five-year Plan. Some observers might argue that such a plan has merely symbolic importance given that the PRC is no longer a planned economy.[20] Indeed, the role of the plan was amended in 1993 to provide more room for

[15] Rogier Creemers, "China's Long and Winding Road in Global Cyberspace: Great Power Relationships or Common Destiny?", *SSRN*, accessed 26 October 2021, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3776814.
[16] Mike Pence, "Vice President Mike Pence's Remarks on the Administration's Policy Towards China", *Hudson Institute*, accessed 26 October 2021, at https://www.hudson.org/events/1610-vice-president-mike-pence-s-remarks-on-the-administration-s-policy-towards-china102018.
[17] Rogier Creemers, "China's Social Credit System: An Evolving Practice of Control", *SSRN*, accessed 26 October 2021, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792.
[18] See, for instance, Lowy Institute, "COVIDcast: the China Story", *Lowy Institute*, accessed 26 October 2021, at https://soundcloud.com/lowyinstitute/covidcast-episode-3-us-china-great-power-competition.
[19] European Commission, "The Digital Services Act package", *European Union*, accessed 26 October 2021, at https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.
[20] Barry Naughton, *Growing Out of the Plan: Chinese Economic Reform*, Cambridge, Cambridge University Press, 1997.

market forces and decentralised decision making. However, the plan continues to serve as administrative guidelines, not least in support of macroeconomic control by means of the strategic allocation of resources. Most importantly, however, a Five-year Plan is more about opening a new "planning cycle" than offering a comprehensive path. Hence, a Five-year plan is a fairly general document approved by the CCP's Central Committee and China's National People's Congress. Following on from the national priorities identified in a Five-year Plan, China drafts and implements its approach through a network of thousands of subplans. These subplans, which are drafted throughout the entire five-year period, often include detailed instructions on implementation for all levels of government. Hence, it is more appropriate to speak of a five-year planning cycle than to think of the Five-year Plan as a cohesive, unified blueprint.[21]

The same need for nuance holds for digital technologies. Technology is all too often dichotomously discussed as either the solution to current problems or the demise of the social values and job security attributed to the "offline" world. In the history of technological transformations, we have seen that new technologies have created better economic opportunities and better living conditions for many, on the one hand, and determined the abandonment of older systems and thus the loss of associated jobs, on the other. In the past, this cycle has nearly always had a smooth transition due to the slow pace of the introduction of new technologies and the abandonment of the old ones. Moreover, those who lost their jobs were often able to be reintroduced into a new area of the economy thanks to the slow evolution of the cycle. However, the current digital revolution is proceeding at impressive speed, and this is creating the risk of threatening social values and job security. It is clear that for those people who are unable to upskill themselves, there will be a concrete risk of marginalisation. Governments will have to devise policies to remedy these risks. Meanwhile, educational institutions will have to rethink themselves to offer life-long learning that can constantly upskill workers. These institutions will have to put more emphasis on the ability to learn than on learning. The tremendous development of technical knowledge and the impossibility of systematising it within traditional knowledge centres such as universities make it likely that companies will have to introduce upskilling courses and training, as it will be hard for them to hire fully "competent" workers. However, not every company will have the strength or ability to introduce these training functions, which will constitute a threat to their survival.

[21] Sebastian Heilmann, *Red Swan: How Unorthodox policymaking facilitated China's Rise*, New York, Columbia University Press, 2018.

How to make sense of China's digital tech ambitions?

To address the implications of China's growing influence by virtue of its digital technologies, we suggest that three elements need to come together: an understanding of China's ambitions, an assessment of the relevance of China's digital policies, and an examination of the feasibility of China's digital agenda. This will require collaboration between technical experts and China scholars.

- *Understanding China's ambitions:* China regularly produces openly accessible information on its digital policies and ambitions. The most prominent of these are legal and regulatory documents, policy plans, speeches by senior officials, and publications by government departments and affiliated think tanks. Local government continues to act as an experimental laboratory for policy ideas that may subsequently be adopted nationally. In addition to such policy documents, technical sources such as technical standards, technical specifications and the strategies of major technology firms also add to our knowledge. There is also considerable debate among social scientists and engineers in China about the future course of the country and the role of technology. The main challenge for the EU is not the lack of available information, but to identify what is important in the enormous quantity of sources that are usually only available in Mandarin Chinese. Machine learning and AI could be helpful as research tools but cannot replace acts of *interpretation* by technical and China experts.
- *Assessing the relevance of China's digital policies:* China's digital technology ambitions also need to be contextualised. At their core, they are a reflection of Chinese domestic concerns and aspirations. Beijing has come to see technology as a magic bullet for resolving perennial policy problems that have plagued the CCP for decades, and as an accelerant of economic growth. Put bluntly, China has recognised that its export-led, low value-added manufacturing-based growth model has run out of steam, and has identified digital industries as a crucial element in a strategy to achieve developed country levels of wealth before demographic headwinds or the middle-income trap kick in. Similarly, digital technologies have been identified by China as a tool for raising its stature internationally. We should, however, be

careful about projecting our own assumptions about global power and the role of technology in its achievement on how China approaches related questions. China's approach might be more modest and transactional than we think, and is predominantly focused on specific economic interests rather than wholesale nation rebuilding. Nonetheless, gains in international power may also play a role.

- *Examining the feasibility of China's digital agenda*: Understanding Chinese technological ambitions and contextualising them within the PRC's political agenda cannot explain or even project actual impacts. For this, the EU needs to assess the extent to which these Chinese viewpoints or ambitions reflect technological possibilities. It is one thing to explain the motivation for the CCP seeking self-sufficiency in semiconductor manufacturing or China's AI ambitions, but quite another to assess whether, and under what conditions, either is feasible. Similarly, an evaluation of the quality of Huawei 5G standard contributions, the technical tools deployed by the Chinese Computer Emergency Response Team or the functioning of China's new blockchain-powered digital currency and Blockchain Service Network requires the collaboration of technical and country experts.

A rigorous analysis based on these three steps can flag emerging trends and provide recommendations. For instance, China's current crackdown on technology companies, which has surprised many observers, was presaged by signals in Chinese policy documents and leaders' speeches.[22] The indigenisation of China's telecommunications infrastructure was already mentioned as a priority in a policy document in 2003.[23]

What Digital Power China consortium has to offer

All this requires teamwork among technical experts and China scholars to provide policy-relevant analysis and concrete recommendations to the EU. Even the highest quality analysis cannot replace political decision making, but it

[22] Zheping Huang, "Xi Warns Against Tech Excess in Sign Crackdown Will Widen", *Bloomberg*, accessed 26 October 2021, at https://www.bloomberg.com/news/articles/2021-03-16/xi-warns-against-tech-excess-in-sign-crackdown-will-widen.

[23] China Copyright and Media, "Opinions concerning Strengthening Information Security Protection Work", *China Copyright and Media*, accessed 26 October 2021, at https://chinacopyrightandmedia.wordpress.com/2003/09/07/opinions-concerning-strengthening-information-security-protection-work/.

can provide factual support to this process. The Digital Power China (DPC) consortium is a diverse group of political scientists, engineers and economists based across Europe. It has come together to offer policy advice to the EU in order to tackle this four-dimensional challenge and promote the ongoing realignment of EU digital technology policy. By serving as a "knowledge hub", the consortium brings together expertise on Chinese and EU policymaking with expertise on digital technologies. It covers nine clusters: *(a)* AI and the IoT; *(b)* blockchain and other secure transactions; *(c)* 5G and beyond: wireless networks; *(d)* strategic hardware and semiconductors; *(e)* cybersecurity and intelligence; *(f)* data governance and disinformation; *(g)* the Digital Green Deal; *(h)* Chinese industrial policy and digital supply chains; and *(i)* technical standardisation and international cyber-governance.

Cooperation across clusters, such as on edge and cloud computing, cures thematic overlap. A particular focus of attention is Chinese direct investment in EU entities and third countries active in digital technologies. The four clusters that engage with specific technologies keep track of Chinese investments related to their respective domains.

Based on thorough academic and policy-oriented research, as well as country-specific expertise that includes Chinese language skills, the consortium: *(a)* assesses the state of Chinese high-tech innovation and rollout, and continuously tracks the rapid development of China's innovation and digital policy, as well as relevant acquisitions and project involvement in Europe and third countries; *(b)* analyses technical relevance and impact against the background of the opaque strategies and structures of China's digital political economy; *(c)* projects short-term trajectories; and *(d)* provides policy advice to the EU.

Summary of chapters

In its first public report, the DPC in collaboration with the China in Europe Research Network (CHERN) is seeking to interact with EU officials on China's digital policies in six specific areas.

In their chapter, Jan-Peter Kleinhans and John Lee argue that Europe is increasingly dependent on Chinese semiconductor manufacturing capacity. This is especially true for the final production steps in semiconductor manufacturing: assembly, testing and packaging. While Europe has tried to incentivise the construction of new wafer fabrication capacity in Europe, this final production step has so far received very little attention from policymakers. The paper argues that an overreliance on Chinese packaging capacity is detrimental to member states' security and Europe's long-term technological competitiveness. The authors suggest several concrete policy actions to strengthen Europe's advanced

packaging ecosystem and close collaboration with allies to ensure long-term technological competitiveness vis-à-vis China.

In their contribution, Liesbet van der Perre and Tim Rühlig discuss some of the challenges in the field of wireless technology following the controversy over the inclusion of Huawei in European 5G networks. They identify slow deployment as a fundamental obstacle to digital innovation in the EU. In addition to addressing the shortage of hardware components, a substantial increase in human resources will be necessary in the long-term. The influx of Chinese researchers based on China Scholar Council funding will need to be discussed in light of potential security risks. Network security risks will require opening up spectrum for private networks in parallel with securing public networks. A more coherent regulatory approach across Europe coupled with investment in European technological strongholds will be essential to avoid the political costs that result from overdependencies. All this leads the authors to opt for a cautious review of EU-China cooperation in the field of wireless technology.

The risk of one-sided dependencies is greater with respect to the IoT than AI, as China has a competitive advantage in the former, Carlo Fischione, Sanne van der Lugt, and Frans-Paul van der Putten argue in their chapter. If the EU sticks to its principle of open markets even though European companies find it difficult to compete with China in the arena of the more advanced technologies, the EU risks to losing these companies and the Chinese government could leverage the dependency created for its political aims.

In their initial exploration, Una Bērziņa-Čerenkova, Elena Ferrari and Julia Vo explore efforts by Chinese government representatives in the EU to influence European public opinion during the 2020 US Presidential elections. Over a four-week period around 3 November 2020, they examine the tweets of 25 Chinese government EU-based Twitter accounts to assess whether there was an enhanced and sustained effort to influence European public opinion on key geopolitical issues. Their analysis identifies Chinese government efforts on Twitter to influence European public opinion on the US, including through proxy references. Further research is required to establish the link between global Chinese government accounts and European-based Chinese government representatives, as well as to test more advanced tools for tweet retrieval, for example through sentiment analysis.

In their chapter on technical standardisation, Tim Rühlig and Maja Björk argue that technical standards setting can translate into power in all four dimensions of the digital China challenge outlined above. China's influence on international standardisation is growing, creating challenges for EU interests in the form of politicisation, the risk of international bifurcation and shifts in power over technical standardisation. The paper makes three sets of policy recommendations on ways forward for an EU

response to China's increased standardisation power. The strategic importance of technical standards, not least in the emerging competition over high technology, means that they will require strategic responses and even greater attention from the EU in the years to come.

The contribution of Maaike Okano-Heijmans and Brigitte Dekker discusses the consequences for the EU of China's digital power projection, especially in China's neighbourhood – a region the EU now calls the Indo-Pacific – and in Europe's own backyard. China's moves require the EU and its member states to adopt an integrated approach that connects the dots between the digital agenda, the connectivity agenda and EU policies on priority regions. The policy recommendations highlighted in this chapter call on the EU to invest in achieving market and standard-setting power, to complement the EU's regulatory power; prioritise the Indo-Pacific region and Africa; develop issue-based cooperation networks and digital governance that put people first; and invest in digital development assistance and capacity building.

Authors:
Rogier Creemers is an Assistant Professor in Modern Chinese Studies at the Leiden Asia Centre in the Netherlands. Contact: r.j.e.h.creemers@hum.leidenuniv.nl
Carlo Fischione is a full Professor of Internet of Things at the KTH Royal Institute of Technology in Sweden. Contact: carlofi@kth.se
Tim Rühlig is a Research Fellow at the German Council on Foreign Relation and an Associate Research Fellow of the Swedish Institution of International Affairs' Europe program. He is based in Germany. Contact: ruehlig@dgap.org


DPC

Europe's dependence on Chinese semiconductor manufacturing

Jan-Peter Kleinhans, John Lee

Abstract

This chapter argues that Europe is increasingly dependent on Chinese semiconductor manufacturing capacity. This is especially true for the final production steps in semiconductor manufacturing: assembly, testing and packaging. While Europe has tried to incentivise the construction of new wafer fabrication capacity in Europe, this final production step has so far received very little attention from policymakers. The chapter argues that an overreliance on Chinese packaging capacity is detrimental to member states' security and Europe's long-term technological competitiveness. The authors suggest several concrete policy actions to strengthen Europe's advanced packaging ecosystem and close collaboration with allies to ensure long-term technological competitiveness vis-à-vis China.

Semiconductors have received considerable attention from policymakers in recent years. They are at the centre of the US-Chinese technology rivalry, and their importance to the automotive industry and many other sectors has become painfully clear during the COVID-19 pandemic and the resulting chip shortages.[24] Several governments have devised plans to invest substantially in their domestic semiconductor industries in order to alleviate current and future supply constraints, strengthen the technological competitiveness of their domestic semiconductor ecosystems and reduce dependence on foreign technology providers.

Europe's efforts in this regard, as set out in the *2030 Digital Compass*,[25] the *Joint Declaration on Processors and Semiconductor Technologies*,[26] and the updated

[24] Jan-Peter Kleinhans and Julia Hess, *Understanding the Global Chip Shortages: Why and How the Semiconductor Value Chain was Disrupted*, Stiftung Neue Verantwortung, November 2021, https://www.stiftung-nv.de/sites/default/files/understanding_the_global_chip_shortages.pdf.

[25] European Commission, *2030 Digital Compass: The European Way for the Digital Decade*, March 2021, https://ec.europa.eu/newsroom/dae/redirection/document/75375.

[26] Joint Declaration, "A European Initiative on Processors and semiconductor technologies", 7 December 2020, https://ec.europa.eu/newsroom/dae/redirection/document/73940.

New Industrial Strategy,[27] are predominantly focused on strengthening capabilities in chip design and front-end fabrication – the first two of the three semiconductor production steps. Increasing the EU's front-end fabrication capacity (building new or expanding existing fabrication plants, or "fabs") has received the most attention from European policymakers. The Digital Compass states that Europe needs to invest in "manufacturing capacities below 5nm nodes aiming at 2nm" within this decade, while the above-mentioned Joint Declaration wants "to strengthen Europe's capabilities to design and eventually fabricate the next generation of trusted, low-power processors".

While Europe's focus on incentivising the construction and expansion of cutting-edge front-end fabs is understandable, it is certainly not the only process step on which Europe is highly dependent on foreign technology providers, specifically China. The third step in semiconductor manufacturing – assembly, test and packaging (ATP), which is also referred to as the "back-end" – has by contrast received little attention from European policymakers. Europe's severe lack of back-end fabs and dependence on Chinese back-end capacity is detrimental to member states' security and long-term economic competitiveness.

This paper first introduces the back-end production steps of semiconductor manufacturing and their increasing importance for future energy efficiency and chip performance. It then reviews the rise of Chinese ATP companies and how Chinese government policies support the development of packaging technology in China. The final section elaborates on why dependence on Chinese back-end capacity creates substantial national security risks and threatens Europe's economic competitiveness.

The role of assembly, test and packaging in semiconductor manufacturing

As noted above, semiconductor manufacturing consists of three distinct steps: chip design, wafer fabrication (front-end), and assembly, test and packaging (or back-end). During wafer fabrication in a front-end fab, integrated circuits are etched on to a wafer using hundreds of chemicals and more than 1000 process steps. During ATP in a back-end fab, the individual integrated circuits (from dozens to hundreds) are tested, cut out of the wafer and encapsulated in protective cases. Wafer fabrication is highly capital intensive with almost insurmountable barriers to market entry at the cutting-edge.[28] ATP, by contrast, has historically been labour intensive with less complicated process steps that rely on cheaper

[27] European Commission, "Updating the 2020 New Industrial Strategy", COM(2021) 350, 2021, https://ec.europa.eu/info/sites/default/files/communication-industrial-strategy-update-2020_en.pdf.

[28] Jan-Peter Kleinhans, "The Lack of Semiconductor Manufacturing in Europe", SNV Policy Paper, April 2021, https://www.stiftung-nv.de/en/node/3045.

equipment, resulting in substantially lower capital expenditure for fabs, lower research and development margins, but also substantially lower value-add compared to chip design and wafer fabrication.[29]

Historically, integrated device manufacturers (IDM), such as Infineon, NXP or ST Microelectronics, took care of ATP in-house in their own back-end fabs. Back-end processes are also often outsourced to foundries such as TSMC or Globalfoundries, however, or to specialist outsourced semiconductor assembly and test (OSAT) companies such as ASE Group or Amkor Technologies.[30]

The economics of back-end manufacturing – relatively labour-intensive with low value-add and narrow profit margins – led increasingly to it being outsourced to China, Taiwan and other countries in Southeast Asia. While the back-end market is substantially less concentrated by market share than cutting edge front-end manufacturing, it is to some extent geographically concentrated. More than 60% of global ATP capacity is currently located in Taiwan and China,[31] which includes the back-end fabs of Western companies located in China and Taiwan.[32] Chinese OSAT companies have been especially successful, growing their global market share to around 20% by 2020.[33]

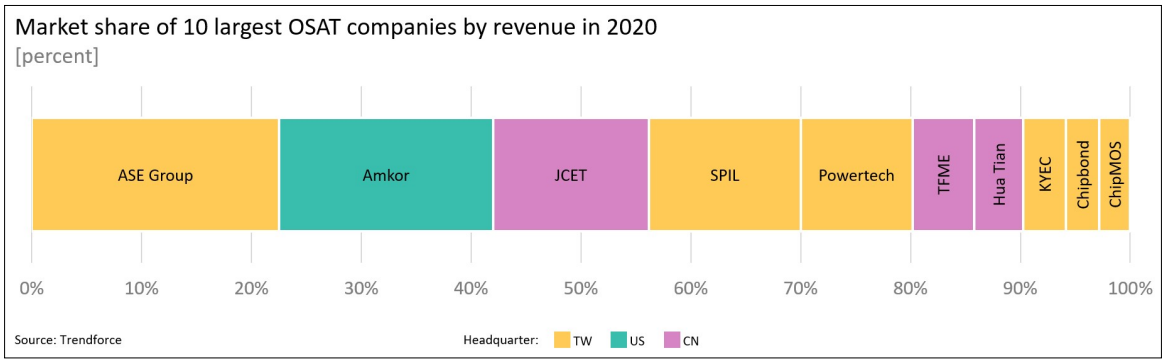

Figure 1: Market share of 10 largest OSAT companies by revenue in 2020 in percent. Source: Own graphic.

[29] Antonio Varas et al., *Strengthening the Global Semiconductor Supply Chain in an Uncertain Era*, Semiconductor Industry Association, April 2021, https://www.semiconductors.org/wp-content/uploads/2021/04/SIA-BCG-Report_Strengthening-the-Global-Semiconductor-Supply-Chain_April-2021.pdf.

[30] Jan-Peter Kleinhans and Nurzat Baisakova, "The Global Semiconductor Value Chain", SNV Policy Paper, October 2020, https://www.stiftung-nv.de/en/publication/global-semiconductor-value-chain-technology-primer-policy-makers.

[31] Semiconductor Industry Association, Public Comment on 86 FR 14308 Semiconductor Manufacturing and Advanced Packaging Supply Chain NOI (Bureau of Industry and Security), Public Comment 79, 6 April 2021, https://www.regulations.gov/comment/BIS-2021-0011-0080.

[32] Like many other Western IDMs and foundries, Infineon, NXP and STMicroelectronics all operate back-end fabs in China.

[33] Manish Nigam et al., "Asia Technology Strategy, China: Can it gain tech independence?" Credit Suisse, 2019.

The rise of Chinese industry in the ATP sector

The back end of the semiconductor value chain is receiving sustained attention from policymakers in China. The Chinese state, from senior leaders in Beijing down through provincial and municipal governments, is focused on promoting coordinated development of the entire value chain, including investment in ATP capacity expansion and technological advances.[34] This presents challenges for Europe – in terms not just of the semiconductor value chain, but also of the multiple industries and technological ecosystems built on it. It has far-reaching implications for national security and the global balance of economic, political and ideational power.

The cost incentives for outsourcing the value chain's back-end to East Asia have had dramatic results. China had become the largest (25%) market for semiconductor packaging materials by 2019, followed by Taiwan, South Korea and Japan.[35] With support from China's state-directed semiconductor industry investment fund, Chinese ATP leaders expanded massively through mergers and acquisitions, while at the same time upgrading their technological capabilities.[36] Further expansion by this path has been blocked by the Taiwanese authorities, however, and in the current geopolitical environment Chinese OSAT firms will need to rely primarily on their own resources and domestic support for any further advances.[37]

"Advanced" packaging techniques, such as heterogeneous integration and 3D stacking, allow chip designers to integrate even more functionality into a single chip, where such functions had previously been separated across multiple chips. Higher levels of integration mean closer proximity to different functionalities and thus higher energy efficiency of the final chip. Numerous advanced packaging techniques are currently being explored by IDMs, foundries and OSATs in an attempt to grow this future market. Advanced packaging still accounts for a minority share of the revenues of Chinese OSAT leaders – by one estimate, around 20%.[38] Nonetheless, these Chinese firms are now pushing the technological frontier in some areas.[39] The leading Chinese firm, JCET, for example,

[34] John Lee and Jan-Peter Kleinhans, "Mapping China's Place in the Global Semiconductor Industry", The Diplomat, 7 September 2021, https://thediplomat.com/2021/09/mapping-chinas-place-in-the-global-semiconductor-industry/.
[35] IHS Markit, "Electronic Chemicals: PCB Chemicals and Semiconductor Packaging Materials", December 2019, https://ihsmarkit.com/products/pcb-chemicals-semiconductor-packaging-materials.html.
[36] John Lee and Jan-Peter Kleinhans, "Mapping China's Semiconductor Ecosystem in Global Context: Strategic Dimensions and Conclusions", MERICS & SNV Policy Paper, 30 June 2021, https://merics.org/en/report/mapping-chinas-semiconductor-ecosystem-global-context-strategic-dimensions-and-conclusions.
[37] Nikkei Asian Review, "Tsinghua Unigroup-SPIL Deal Axed on Policy Worries", 28 April 2016, https://asia.nikkei.com/Business/Tsinghua-Unigroup-SPIL-deal-axed-on-policy-worries.
[38] Litho World, "Current Status of the Integrated Circuit Industry in China: IC Manufacturing Industry", December 2019, https://www.researchgate.net/publication/338341090_Current_Status_of_the_Integrated_Circuit_Industry_in_China_-_Packaging_and_Testing_Industry_Review.
[39] Litho World, "Current Status of the Integrated Circuit Industry in China: IC Manufacturing Industry",

which is now the third largest packaging firm globally by sales, employs cutting-edge techniques such as 2.5 & 3D (heterogenous) packaging.[40]

Chinese OSAT leaders can profitably expand their capacity and R&D activities thanks to demand for semiconductors from the wider Chinese economy for applications such as 5G telecoms infrastructure, electric vehicles and consumer electronics. Due to the way in which these firms have expanded, they also enjoy established relations with US customers, such as chip design leader AMD, which further buttresses their revenue base.[41] China's OSAT leaders are all reportedly planning secondary public offerings to raise capital to invest in capacity expansion and advanced packaging techniques.[42]

Chinese OSAT leaders will also benefit from the local concentration of the *printed circuit board (PCB) substrate industry***.** PCBs are the internal "mounting plates" for all the chips and semiconductors in an assembled electronic system.

While PCB manufacturers are not considered semiconductor companies, they play a crucial role in the electronics industry. The PCB industry is increasingly closely related to the semiconductor value chain's back-end, as performance demands in consumer electronics drive PCB vendors to pursue miniaturisation.[43] The global PCB supply chain is now concentrated in China, and Chinese suppliers are growing their share in a market dominated by Taiwanese, South Korean and Japanese firms.[44] In 2019, China accounted for over half the global market for the chemicals used in PCB production, and was the fastest growing market followed by Taiwan and South Korea.[45]

In this context, Chinese OSAT leaders are well placed to pursue advanced packaging. Advanced packaging techniques are being promoted by Chinese industry experts as an alternative to the increasing technical difficulty of shrinking fabrication nodes that is implied by "Moore's Law", which is now approaching its physical limits. This technical difficulty is a

December 2019, https://www.researchgate.net/publication/338341090_Current_Status_of_the_Integrated_Circuit_Industry_in_China_-_Packaging_and_Testing_Industry_Reviewe.

[40] Henrik Bork and Michael Eckstein, "Neue Ära: China setzt auf Advanced Packaging und Testing", Elektronik Praxis, 20 April 2021, https://www.elektronikpraxis.vogel.de/neue-aera-china-setzt-auf-advanced-packaging-und-testing-a-1016761/.

[41] TrendForce, "Revenue of top 10 OSAT companies for 2Q21 reaches US$7.88 billion due to strong demand and increased package/test prices, says TrendForce", 6 September 2021, https://www.trendforce.com/presscenter/news/20210906-10926.html.

[42] Henrik Bork and Michael Eckstein, "Neue Ära: China setzt auf Advanced Packaging und Testing", Elektronik Praxis, 20 April 2021, https://www.elektronikpraxis.vogel.de/neue-aera-china-setzt-auf-advanced-packaging-und-testing-a-1016761/.

[43] IHS Markit, "Electronic Chemicals: PCB Chemicals and Semiconductor Packaging Materials", December 2019, https://ihsmarkit.com/products/pcb-chemicals-semiconductor-packaging-materials.html; Pinsheng Electronics, "Substrate-like PCB: The highlight in the future PCB industry", 13September 2021, https://www.quick-pcba.com/pcb-news/substrate-like-pcb-technology.html.

[44] Macquarie Research, "China PCB sector: Growing dominance in the 5G era", 2019.

[45] IHS Markit, 2019, "Electronic Chemicals: PCB Chemicals and Semiconductor Packaging Materials", December 2019, https://ihsmarkit.com/products/pcb-chemicals-semiconductor-packaging-materials.html.

critical bottleneck for China's semiconductor industry, and advanced packaging is being pursued as an alternative pathway, for example at SMIC, China's leading foundry.[46]

The imposition of US export controls on SMIC – and SMIC's inability to acquire certain advanced machinery (such as an EUV stepper from the Dutch equipment maker, ASML) that is indispensable for recent generation fabrication nodes – has highlighted the imperative for China's semiconductor industry as a whole to seek alternative technical pathways simply to keep pace with technological progress, and to mitigate the risk that foreign "decoupling" measures could choke off Chinese industry's capacity to continue to advance semiconductor performance.

With little prospect of catching the global leaders in front-end fabrication – TSMC, Samsung and Intel – through node shrinkage, SMIC is likely to focus instead on advanced packaging.[47] This is reflected in SMIC's most recent round of investments, which includes a 12-inch wafer and packaging project that commenced construction in January 2021.[48] The incentives steering Chinese firms towards advanced packaging are reinforced by government policy, which at senior levels now appears to be focused on "post-Moore" technical approaches in order to circumvent the constraints on Chinese industry.[49]

Chinese state policy: pushing technological advances and the development of an integrated value chain

China's 14th Five-year Plan (FYP), which was launched in March 2021, lists semiconductors as one of seven "frontier technologies" prioritised for national breakthroughs. Although the FYP makes no direct reference to advanced packaging techniques, these are likely to feature in the anticipated 14th Five-year Plan for Science and Technology Innovation, currently being developed by China's Ministry of Industry and information Technology, which will implement the FYP's strategic guidance in more specific terms. Advanced packaging should also be

[46] Iris Deng, "China must pursue chip assembly, packaging breakthroughs to catch up with semiconductor leaders, experts say" South China Morning Post, 9 June 2021, https://www.scmp.com/tech/policy/article/3136688/china-must-pursue-chip-assembly-packaging-breakthroughs-catch; Che Pan, "SMIC urges China's chipmakers to embrace advanced packaging as Moore's Law slows nanometre node progress and US sanctions bite", South China Morning Post, 25 January 2021, https://www.scmp.com/tech/big-tech/article/3119174/smic-urges-chinas-chipmakers-embrace-advanced-packaging-moores-law.

[47] Tim Culpan, "An $11 Billion Distraction for China's Chip Ambitions", Bloomberg, 6 September 2021, https://www.bloomberg.com/opinion/articles/2021-09-06/china-is-pouring-billions-of-dollars-into-old-chip-technology.

[48] EET China, "半导体一周要闻 - 莫大康", 2021, https://www.eet-china.com/mp/a75048.html.

[49] Minghe Hu, "China wants to boost disruptive semiconductor technologies as Moore's Law moves towards its limit", South China Morning Post, 15 May 2021, https://www.scmp.com/tech/article/3133613/china-wants-boost-disruptive-semiconductor-technologies-moores-law-moves.

expected to appear in a potential new Medium- to Long-term Plan for Science and Technology Development, which will supersede its 2006–2020 iteration.[50]

These plans will probably be accompanied by one or more new national "special projects" on semiconductor R&D, which would be successors to two such 15-year projects that concluded in 2020. These special projects brought together research institutes, state-owned enterprises and private sector companies in efforts to plug capability gaps in China's domestic industry and develop new technologies. They included several items concerned with packaging technology. China's three leading ATP firms participated in these projects, assisting their progress in advanced packaging techniques.

Semiconductor industry development plans are being promulgated by many of China's sub-national governments, and many of these plans emphasise packaging technologies. For example, the City of Shanghai and Jiangsu Province – both important centres of China's semiconductor industry – are promoting ATP and specific advanced packaging techniques in their 14th FYP implementation plans.[51] These plans emphasise coordinated and holistic development of the semiconductor value chain and aim to create synergies between different steps to mutually catalyse technological progress.

This approach is backed by China's state-directed investment fund for the semiconductor sector – the Big Fund. The goal, to quote the Big Fund's manager, is to "increase cooperation between domestic enterprises, truly realise upstream and downstream integration, and create a virtual IDM [integrated device manufacturer] model".[52] In light of enhanced measures by the US government to restrict Chinese firms' access to semiconductor-related technologies and equipment, leaders in Beijing perceive that long-term national economic security depends on building up the capacities of domestic industry throughout the value chain, of which back-end processes are an indispensable element.

In this context, Beijing will seek to shape the evolution of the global packaging sector, including through measures that support Chinese firms and potentially discriminate against foreign ones, in the service of national strategic objectives. President Xi Jinping has said that China must "pull tight" international supply chains, and practice punitive deterrence against attempts by foreigners to

[50] John Lee and Jan-Peter Kleinhans, "Mapping China's Place in the Global Semiconductor Industry", The Diplomat, 7 September 2021, https://thediplomat.com/2021/09/mapping-chinas-place-in-the-global-semiconductor-industry/.

[51] Shanghai Municipal Government, "14th Five-Year Plan for the Development of Advanced Manufacturing Industry in Shanghai" (in Chinese), 2021, https://www.shanghai.gov.cn/nw12344/20210714/0a62ea7944d34f968cbc49eec47dbca.html; Jiangsu Provincial Government, "The 14th Five-Year Plan of Nanjing's Jiangbei New Area" (in Chinese), 2021, http://www.jiangsu.gov.cn/art/2021/8/23/art_46144_9984347.html.

[52] East Money Securities, "The Big Fund's First Phase investments have been most fruitful, Phase Two is ready for launch" (in Chinese), 2019, http://data.eastmoney.com/report/zw_industry.jshtml.

interrupt Chinese industry's supply chains.[53] European strategic planning must account for this holistic and increasingly adversarial mindset that is guiding Chinese industrial policy, and for the implications of the concentration in China of seemingly innocuous and – for the time being – relatively low value-added back-end processes for manufacturing semiconductors.

The risks of overreliance on Chinese back-end manufacturing

Reliance on Chinese OSAT companies and back-end fabs in China creates potential *national security challenges.* Packaging is the most viable production step for an adversary to compromise a chip by hiding additional functionality in it, such as a hardware "backdoor" or a "kill switch".[54] This national security dimension is the reason why the US government's 100-day supply chain review for semiconductors, finalised in June 2021, specifically includes the mapping of dependencies and potential vulnerabilities in the packaging supply chain.[55] Domestic front-end fabs do not alleviate this risk. Even if wafer fabrication is carried out domestically, if the finished wafers are sent to China for ATP the chips could still be compromised during the packaging processes.[56]

There is a further *economic challenge* for the European semiconductor ecosystem if it lacks technological competitiveness in advanced packaging. Improvements in advanced packaging, such as heterogeneous integration, will play a critical role in future chip design.[57] While semiconductor manufacturing was historically all about improvements in the fabrication process (front-end fabs), these improvements now have diminishing returns – the "death" of Moore's Law.[58] Thus, companies are focused more and more on innovations in packaging to make chips more energy efficient and more powerful.[59] While Europe is strong in advanced

[53] Qiushi, "General Secretary Xi Jinping: Industry chains and supply chains must not fall off at critical times" (in Chinese), 2020, http://www.qstheory.cn/zhuanqu/2020-11/03/c_1126690768.htm .
[54] John Lee and Jan-Peter Kleinhans, "Mapping China's Semiconductor Ecosystem in Global Context: Strategic Dimensions and Conclusions", MERICS & SNV Policy Paper, 30 June 2021, https://merics.org/en/report/mapping-chinas-semiconductor-ecosystem-global-context-strategic-dimensions-and-conclusions.
[55] The White House, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth*, 100-Day Reviews under Executive Order 14017, June 2021, https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf
[56] Tiago Perez and Samuel Pagliarini, "A Survey on Split Manufacturing: Attacks, Defenses, and Challenges", 7 October 2020, https://doi.org/10.1109/ACCESS.2020.3029339.
[57] IEEE, "Heterogeneous Integration Roadmap, Chapter 2: High Performance Computing and Data Centers", October 2019, https://eps.ieee.org/images/files/HIR_2019/HIR1_ch02_hpc.pdf.
[58] Samuel K. Moore, "A better way to measure progress in semiconductors", *IEEE Spectrum*, 21 July 2020, https://spectrum.ieee.org/a-better-way-to-measure-progress-in-semiconductors.
[59] IEEE, "Heterogeneous Integration Roadmap", 2021 Symposium, 2019 edition, https://eps.ieee.org/technology/heterogeneous-integration-roadmap.html.

packaging R&D,[60] it has a severe lack of domestic packaging capacity.

Increased reliance on Chinese back-end services would provide a supply chain chokepoint through which Beijing could exert *political pressure* of the kind used against Sweden, Germany and other EU member states concerning Huawei and 5G networks.[61] China's new counter-sanctions law – and the scope for retaliation against foreign actions that is provided for in Chinese legislation such as the Foreign Investment Law and Data Security Law, which likewise can be exercised with extraterritorial jurisdiction – indicate that Beijing intends increasingly to have the option of directly punishing foreign businesses, to shape development of transnational technological ecosystems such as the semiconductor value chain in ways that favour Chinese firms.[62]

Finally, a global economy in which Chinese firms shape technological ecosystems *will present ideational challenges* for Europe. As the European Commission's Strategic Foresight Report puts it, "setting favourable conditions across the value chain" is essential to the EU's capacity and freedom to act on the global stage.[63] If Chinese firms take the lead in advanced packaging, this will have advantageous flow-on effects for China's wider semiconductor sector and other industry verticals, such as the automotive sector as it transitions to increasingly electrified and computerised vehicles.

This will erode European firms' competitiveness along the semiconductor value chain and in the many industry verticals that depend on it, which in turn means diminished influence vis-à-vis Beijing's regulatory and political preferences. Ideational power as expressed in technological ecosystems is based on economic competitiveness and market share. For example, advanced packaging capabilities in China could support local development of AI accelerators and hence Chinese-developed AI solutions. These products would be shaped by the Chinese state's frameworks for data regulation and ethical governance of AI, which could displace European approaches in these fields internationally if Chinese products enjoy a competitive advantage linked to the underlying domestic semiconductor ecosystem.

More immediately, the Chinese authorities are increasingly involving themselves in domestic supply chain mapping and management, and increasingly requiring extensive data exchanges with

[60] The leading semiconductor research and technology organisations (RTO) in Europe – CEA-Leti, Fraunhofer and imec – are all heavily invested in cutting-edge advanced packaging and heterogeneous integration research.

[61] Politico, "Sweden faces Chinese blowback over Huawei ban", 21 January 2021, https://www.politico.eu/article/sweden-faces-chinese-blowback-over-huawei-ban/.

[62] Katja Drinhausen and Helena Lagarda, "China's Anti-Foreign Sanctions Law: A warning to the world", MERICS, 24 June 2021, https://merics.org/en/short-analysis/chinas-anti-foreign-sanctions-law-warning-world.

[63] European Commission, "2021 Strategic Foresight Report: Enhancing the EU's long-term capacity and freedom to act", COM(2021) 750, 2021, https://ec.europa.eu/info/sites/default/files/foresight_report_com750_en.pdf.

industry.[64] These impositions will be made unavoidable for European actors by the packaging sector's concentration in China, which will increasingly challenge European preferences regarding appropriate levels of government intervention in private sector business operations. It will also expose European interests to growing visibility and exercise of leverage on the part of the Chinese authorities, which is likely to be wielded in the service of Chinese political priorities.

Unfortunately, ATP does not play any role in Europe's semiconductor strategy as laid out in the 2030 Digital Compass and the Joint Declaration on Processors and Semiconductor Technologies. The strong focus on incentivising semiconductor companies to invest in cutting-edge front-end fabs in Europe ignores the fact that finished silicon wafers would still need to be shipped to Taiwan or China for assembly, test and packaging. It also underestimates the importance of advanced packaging and heterogeneous integration to future chip development, and hence its importance to the European semiconductor ecosystem in gaining technological leadership.

Conclusions and recommendations for Europe

While Europe is right to invest in front-end fabs, this should not be the sole focus of the EU's semiconductor strategy. Europe and its semiconductor manufacturers are already heavily dependent on Chinese back-end capacity, a dependence that presents a potential national security threat and threatens a loss of technological competitiveness. Europe would do well to invest in its back-end capacity in the same way that it is currently incentivising the construction of front-end fabs. Four immediate recommendations to strengthen Europe's position and competitiveness in the semiconductor packaging sector are set out below.

- *Incentivise the construction of new and the expansion of existing back-end fabs, with a focus on advanced packaging capabilities*. The IPCEI Microelectronics 2 should be used not only to subsidise the construction of front-end fabs, but also to strengthen back-end capacity. The focus should be on advanced packaging and heterogeneous integration.
- *Include advanced packaging in EU monitoring initiatives:* The new EU Observatory for Critical Technologies should monitor China's role in the global semiconductor value chain, including advanced packaging.[65] Information-sharing channels should be put in place with other

[64] See e.g. "Jiangmen City Bureau of Industry and Information Technology: Concerning the issuance of the 'work plan on ensuring the stability of industrial and supply chains"', 2021, http://www.jiangmen.gov.cn/bmpd/jmsgyhxxhj/ywfl/ghyyxjck/content/post_2071311.html (in Chinese).

[65] European Commission, "Action Plan on synergies between civil, defence and space industries", COM(2021) 70, 2021, https://ec.europa.eu/info/sites/default/files/com-2021-70_en_act_part1_v8_en.pdf.

European monitoring initiatives on Chinese technology policy, espionage and corporate activity.

- *Strengthen cooperation with international partners in advanced packaging:* The Japanese government is subsidising construction of a joint advanced packaging R&D centre together with TSMC, and Japanese equipment vendors and chemical suppliers.[66] In their current conversations with international technology providers such as Intel and TSMC, European governments should devise long-term strategic partnerships on advanced packaging and heterogeneous integration. Back-end fabs are significantly less expensive than front-end fabs with substantially lower barriers to market entry, making them ideal candidates for joint investment.
- *Discuss advanced packaging with the Biden administration in the new EU-US Trade and Technology Council:* "supply chain security" and "ICT security and competitiveness" are among the designated topics for discussion by the Council, which met for the first time on 29 September 2021.[67] The advanced packaging R&D being conducted by US companies with the support of the US Department of Defense provides a potential focus for these discussions.[68]

The packaging sector is just one example of how China's growing prominence in the global semiconductor value chain is raising critical issues for European policymakers. Various open and emerging questions can only be addressed by combining a deep technical understanding of the semiconductor sector with expertise on China's political economy and policy priorities. This combined skillset provides the best foundation on which to build analyses of China's changing role in the global semiconductor ecosystem, and of how best to strengthen Europe's semiconductor sector in response while also positioning Europe in the context of deepening US-Chinese global rivalry over critical technologies. This should not be a short-term or one-off exercise but requires an ongoing commitment to supporting high-quality research that brings together technology- and China-oriented analysts. In an increasingly competitive international environment, policymakers would be well served by access to an accurate and dynamic picture of China's role in the semiconductor value chain and its impacts on European interests.

[66] Phil Garrou, "TSMC Considering Chip Packaging in Japan; US "On Shoring" Report Issued", 3D Incites, 3 August 2021, https://www.3dincites.com/2021/08/iftle-493-tsmc-considering-chip-packaging-in-japan-us-on-shoring-report-issued/.

[67] European Commission, "Trade and Technology Council: US and EU announce inaugural meeting", Press release, 9 September 2021, https://trade.ec.europa.eu/doclib/press/index.cfm?id=2298.

[68] NSTXL, "DoD and S2MARTS Impacting the Microelectronics Ecosystem through the Rapid Assured Microelectronics Prototypes–Commercial (RAMP-C) Project" [n.d.], https://nstxl.org/dod-and-s2marts-impacting-the-microelectronics-ecosystem-through-the-rapid-assured-microelectronics-prototypes-commercial-ramp-c-project/.

Authors:
Jan-Peter Kleinhans is the Director of Technology and Geopolitics at Stiftung Neue Verantwortung in Germany. Contact: jkleinhans@stiftung-nv.de
John Lee is Director of East-West Futures and was formerly a Senior Analyst with the Mercator Institute for China Studies (MERICS). Contact: johnlee@eastwestfutures.com

Wireless networks and EU-China relations beyond the "Huawei debate": Is China a partner, competitor or systemic rival on 5G and 6G?

Liesbet van der Perre, Tim Rühlig

Abstract

Where does Europe stand following the controversy over the inclusion of Huawei in European 5G networks? This chapter reflects on the deployment and development of wireless technology. The authors identify slow deployment as a fundamental obstacle to digital innovation in the EU. In addition to addressing the shortage of hardware components, a substantial increase in human resources will be necessary in the long-term. The influx of Chinese researchers based on China Scholar Council funding should be discussed in light of potential security risks. Network security risks will require opening up spectrum for private networks in parallel with securing public networks. A more coherent regulatory approach across Europe coupled with investment in European technological strongholds will be essential to avoid the political costs that result from overdependencies. All this leads the authors to opt for a cautious review of EU-China cooperation in the field of wireless technology.

The controversial question of whether to include equipment made by the Chinese technology firms Huawei and ZTE in the rollout of Europe's fifth generation mobile technology infrastructure, better known as 5G, has been high up the political agenda for the past two years.[69] In response, the European Union (EU) has developed a "toolbox" to mitigate a wide set of security concerns, including malign foreign influence;[70] and the EU member states are currently

[69] Tim Rühlig and Maja Björk, "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe," *UI Paper 1/2020*, Stockholm, The Swedish Institute of International Affairs, 2020.

[70] NIS Cooperation Group, *Cybersecurity of 5G Networks. EU Toolbox of Risk Mitigation Measures. CG Publication 01/2020*, Brussels, European Commission, 2020.

implementing this toolbox.[71] Nonetheless, in spite of all the progress that Europe has made in this central field of the digital transformation, a number of challenges remain. These challenges occur in the four dimensions that the Digital Power China consortium refers to as the four dimensions of the "digital China challenge".

Economically, the EU is struggling to address the shortcomings linked to a much slower deployment compared to the People's Republic of China (PRC), which is a frontrunner in the rollout of 5G. In terms of *security,* not even the most drastic action, the exclusion of Chinese vendors, can resolve the vulnerabilities. The handling of *political* dependencies requires a higher degree of unity than the EU has achieved so far, and greater investment in the EU's strongholds. Finally, the PRC is one of the most innovative countries in the development of 5G. This means that the EU needs to consider how to cooperate with an authoritarian country despite its *ideational* differences. This paper discusses these four dimensions, provides concrete policy advice and explores how to shape the role of China, in its relations with the EU, as simultaneously a partner, a competitor and a systemic rival.[72]

Untapping economic potential: catching up with China's deployment

The transformative potential of 5G cannot be overestimated. It should be noted that while in the past, new generations of mobile networks have been numbered, several consecutive standard releases defined by the Third Generation Partnership Project (3GPP)[73] that are categorised as 5G (now called 'New Radio'). Wireless mobile technology infrastructure is a critical enabler of the digital transformation that will penetrate all aspects of Europe's future society and economy. Unlike the transition from 3G to 4G/LTE, 5G does not just have the ambition to increase upload and download capacities, widely known as enhanced mobile broadband (eMBB). The most advanced version of 5G, referred to as standalone 5G (SA 5G), will also make possible progress on supporting the ultra-reliable low latency communication (URLLC) that assists new applications such as vehicle-to-vehicle communications for self-driving cars. In addition, later releases of SA 5G aim to accommodate the connection of a much greater number and diversity of devices, known as massive machine type communication (mMTC). This will trigger a new wave of automation in production by means of machine-to-machine communication and enable the penetration

[71] NIS Cooperation Group, *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*, Brussels, NIS Cooperation Group, 2020.

[72] European Commission, *EU-China - A Strategic Outlook. European Commission and HR/VP Contribution to the European Council. 12 March 2019*, Brussels, European Commission, 2019.

[73] https://www.3gpp.org/specifications/67-releases, Releases 15 and 16 had been finalised at the time of writing while the future releases 17 and 18 will also be considered 5G under consideration.

of wireless connectivity into all spheres of private and societal life, such as smart homes or smart health.

Wireless mobile infrastructure alone is not enough to untap this digital transformation, but it is its backbone. SA 5G is a necessary but not sufficient precondition for creating an ecosystem that is conducive to digital innovation and transformation. Hence, the early deployment of 5G is critical to European competitiveness at a time of digital transformation.

In comparison to the PRC, the EU is far behind in the deployment of public 5G networks, but it is catching up. As of March 2021, only Lithuania, Malta and Portugal had not launched 5G services.[74] South Korea, the US and China are still ahead of the EU. As an early adopter, the PRC claimed to account for 80% of the world's total 5G connections and 70% of global 5G base station deployment as of mid-2021.[75] In contrast to the early local deployments in the US and the EU, China had focused on wide coverage of SA 5G. The PRC has more per capita 5G subscriptions than the US, which is ahead of the EU.[76] In comparative policy planning terms, China's 14th Five-year Plan is more ambitious than the EU's Digital Compass, and aims to achieve full 5G network coverage in urban and rural areas five years before Europe (2025 rather than 2030).[77] In mid-July, ten state organs specified that the PRC is striving to exceed 560 million 5G users by 2023, accounting for more than 40% of all personal mobile phone connections.[78] While these figures emphasise the urgent need for the EU to act, they ignore the fact that the EU could still catch up in the area of private 5G networks, which will be of increasing importance in the deployment and innovation potential of SA 5G. While the EU's Digital Compass does not set clear targets in this area, China promises a penetration of all major industrial companies well above 35% by 2023.[79]

There are multiple reasons for the EU's delay, such as the lack of clarity about

[74] 5G Observatory, "Announcements of Commercial Launches," *5G Observatory*, accessed 30 October 2021, at https://5gobservatory.eu/market-developments/5g-services/.
[75] People's Republic of China, "Goal for 2023: 560 Million 5G Users in Nation," *State Council*, accessed 30 October 2021, at http://english.www.gov.cn/statecouncil/ministries/202107/14/content_WS60ee1a81c6d0df57f98dcce7.html.
[76] Dan Strumpf, "U.S. vs. China in 5G: The Battle Isn't Even Close," *Wall Street Journal*, accessed 30 October 2021, at https://www.wsj.com/articles/u-s-vs-china-in-5g-the-battle-isnt-even-close-11604959200.
[77] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 2030 Digital Compass: the European Way for the Digital Decade. COM(2021) 118 final," *European Commission*, accessed 2 April 2021, at https://ec.europa.eu/info/sites/info/files/communication-digital-compass-2030_en.pdf; Xinhua, "（两会受权发布）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*, accessed 3 April 2021, at http://www.xinhuanet.com/2021-03/13/c_1127205564.htm.
[78] People's Republic of China, "Goal for 2023: 560 Million 5G Users in Nation," *State Council*, accessed 30 October 2021, at http://english.www.gov.cn/statecouncil/ministries/202107/14/content_WS60ee1a81c6d0df57f98dcce7.html.
[79] Ibid.

whether Chinese vendors should be excluded from the EU market, which has left mobile operators reluctant to invest in 5G networks,[80] the late allocation of spectrum, and cumbersome and expensive auctions in many EU member states.[81] In both Japan and China, operators were only required to justify the need to be allocated spectrum but were not charged fees.[82] The partial replacement of Chinese equipment from existing mobile infrastructure in Europe will add costs for mobile operators.[83] However, if the main challenges for Europe had been financial resources and legal clarity, the EU's recovery fund coupled with the adoption of regulation regarding Chinese vendors would have gone a long way to resolving these issues.

Currently, shortages of hardware components – particularly semiconductors – and of human resources are main bottlenecks that the EU faces. It should be noted that essential innovations are required in several key new 5G technologies in order to reach the specifications adopted by the International Telecommunication Union (ITU). One of these is massive MIMO technology, which allows much higher efficiency to be achieved in the frequency bands below 6GHz. Of particular interest is Time Division Duplex (TDD)-based massive MIMO, which operates in the 3.5GHz band reserved for 5G deployment. Interestingly, European researchers and companies have been pioneers in this technology, from both a theoretical[84] and a validation perspective,[85] and great progress was made towards efficient transmission, for example, in the pre-5G EU seventh framework program-funded project MAMMOET.[86] This leading knowhow in Europe has a clear strategic value. Another new approach in 5G is that spectrum in the millimeter wave (mmwave) bands, in particular around 28 GHz and 38 GHz, will be used in the Radio Access Network (RAN). While these bands offer high bandwidth, they pose significant challenges in terms of the deployment, production and design of hardware.[87] The latter in

[80] Supantha Mukherjee and Isla Binnie, "Analysis: Europe Plts Catch-up in Global 5G Race to Drive COVID-19 Recovery," *Reuters*, accessed 30 October 2021, at https://www.reuters.com/article/us-europe-5g-analysis-idUSKBN2920WJ.

[81] ERT, "Assessment of 5G Deployment Status in Europe," *European Round Table for Industry*, accessed 30 October 2021, at https://euagenda.eu/upload/publications/001905-20-205g-20roll-20out-20in-20europe-20paper-20-20s7v1.pdf.pdf.

[82] Ericsson, "Optimizing Spectrum Assignments to Deliver Expansive 5G Connectivity," *Ericsson*, accessed 30 October 2021, at https://www.ericsson.com/49a010/assets/local/policy-makers-and-regulators/optimizing-spectrum-assignments-to-deliver-expansive-5g-connectivity.pdf.

[83] Xuewu Gu et al., *Geopolitics and the Global Race for 5G. CGS Global Focus*, Bonn, Center for Global Studies Bonn, 2019.

[84] E. G. Larsson, O. Edfors, F. Tufvesson and T. L. Marzetta, "Massive MIMO for next generation wireless systems," in *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186-195, February 2014, doi: 10.1109/MCOM.2014.6736761.

[85] J. Vieira *et al.*, "A flexible 100-antenna testbed for Massive MIMO," *2014 IEEE Globecom Workshops (GC Wkshps)*, 2014, pp. 287-293, doi: 10.1109/GLOCOMW.2014.7063446.

[86] https://mammoet-project.technikon.com/

[87] E. Bjornson, L. Van der Perre, S. Buzzi and E. G. Larsson, "Massive MIMO in Sub-6 GHz and mmWave: Physical, Practical, and Use-Case Differences," in *IEEE Wireless Communications*, vol. 26, no. 2, pp. 100-108, April 2019, doi: 10.1109/MWC.2018.1800140

particular requires highly skilled personnel. A quick look at the jobs pages of both smaller and larger European companies innovating mmwave products confirms the scarcity of qualified and experienced personnel. If Europe is to continue to play a leading role, it will need appropriately skilled people.

Hence, the EU needs to sustain strategic leading technological expertise on future network technologies on its territory. This will mean encouraging and stimulating more young Europeans to engage in the engineering studies that are key to the digital society of our futures. As our *first policy recommendation*, we suggest supporting and scaling-up existing initiatives that aim to attract interest in engineering sciences among European youth through education, campaigns and cooperation with the corporate sector to address this structural challenge in the long run. Member states should swiftly allocate spectrum and reduce existing barriers in order to speed up European rollout, which is a precondition for digital transformation and innovation.

Mitigating security risks: facilitating diversification

The security of the EU's 5G networks has been at the core of recent debate, in particular on the challenges that arise from the use of Chinese vendor equipment.[88] Network security challenges focus on concerns over the sabotage of 5G networks and espionage through 5G infrastructure.[89]

Sabotage refers to the risk of a "kill switch" and the idea that Europe's 5G networks could be shut down either fully or partially by a malign actor. Since China and the EU are not in a security alliance, the PRC could constitute such a malign actor. A kill switch could be perceived as a new type of act of war, since in the light of the wide range of applications outlined above shutting down the wireless mobile infrastructure would affect all spheres of public and private life. There is a broad consensus among engineers and hackers that China is capable of network sabotage, and that it is impossible to fully secure the networks against an attack by the PRC. However, the EU can act to increase the cost of a kill switch for China and other malign actors. Critics of Huawei argue that the inclusion of Chinese vendor equipment makes sabotage easier for the PRC.[90] Ironically, however, vendor

[88] Huawei Cyber Security Evaluation Centre Oversight Board, "Annual Report," *HCSEC*, accessed 9 August 2019, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

[89] David Bond and James Kynge, "China Spying Risk Hits Huawei's UK Ambitions," *Financial Times*, 3 December 2018.

[90] Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," *Wall Street Journal*, accessed 27 February 2020, at https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

diversity coupled with network redundancies is widely acknowledged to be the most effective way of increasing the cost of a kill switch.[91] The exclusion of Chinese vendors Huawei and ZTE reduces the number of suppliers in the highly concentrated RAN market.[92]

The risk of a kill switch should also be carefully considered in attempts to upgrade government agency and emergency services communications, largely based on terrestrial trunked radio (TETRA) in Europe, and to leverage 4G and 5G technology. While such a transformation is necessary, how to make such communications secure and reliable will require careful investigation, in particular in connection with redundancy in the networks.

Espionage remains a major risk, not least because China is believed to be responsible for the vast majority of cyberespionage globally.[93] Thus far, most espionage has been carried out not through infrastructure, but by means of applications, phishing and infiltration. These present real challenges. Consider only the large number of Chinese PhD students with scholarships from the China Scholarship Council (CSC) in European universities and research institutions. In some European research teams focusing on wireless communications, the majority of the PhD student are SC scholarship holders, which creates financial dependencies. In addition, Chinese nationals are required by law to cooperate with the Chinese intelligence services if requested.

With new use cases and greater complexity, 5G infrastructure could develop into yet another attack vector in the future.[94] There is a consensus that it is not the exclusion of vendors, but encryption that is the best means for tackling espionage. However, encryption also obstructs the lawful interception of communications, thereby hindering crime prevention and detection.[95]

While in tackling the risk of espionage there will always be a need to balance data security and the legitimate interests of lawful interception, the solution to sabotage lies in the facilitation of diversity and flexibility. Hence, *our second policy recommendation* is to improve the conditions for the flexible and diverse deployment of wireless mobile

[91] Deutscher Bundestag, "Experten gegen Ausschluss von Anbietern beim Mobilfunkstandard 5G. 22 November 2019," *Deutscher Bundestag*, accessed 28 March 2020, at https://www.bundestag.de/dokumente/textarchiv/2019/kw46-pa-auswaertiges-5g-665414; Mathieu Duchâtel and Francois Godement, *Europe and 5G. The Huawei Case*, Paris, Institut Montaigne, 2019.

[92] Jeffrey D. Sachs, "America's War on Chinese Technology," *Project Syndicate,* November 7, 2019, at https://www.project-syndicate.org/commentary/cheney-doctrine-us-war-on-chinese-technology-by-jeffrey-d-sachs-2019-11.

[93] Kadri Kaska et al., *Huawei, 5G and China as a Security Threat*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2019.

[94] Jan-Peter Kleinhans, *5G vs. National Security. A European Perspective*, Berlin, Stiftung Neue Verantwortung, 2019.

[95] Council of the European Union, "Law Enforcement and Judicial Aspects Related to 5G. 8983/19, May 6, 2019," *Council of the European Union*, accessed 30 October 2021, at https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf.

infrastructure. Opening up the spectrum for private wireless networks and creating favourable ecosystems will be crucial, not least because we expect private networks to become more influential over the course of 5G deployment, and the reinforcement of that trend in the next generation of wireless technology, 6G.

A difficult issue is the promotion of the concept of OpenRAN. On the one hand, OpenRAN facilitates diversification because it provides a basis for the components of different suppliers to be interoperable. This contrasts with the proprietary solutions of a small number of vendors. On the other hand, RAN technology is too complex to be subject to constant comprehensive security review by the authorities; hence, the need to trust vendors.[96] OpenRAN solutions require us to trust all contributors while proprietary solutions need only trust in single vendors such as Ericsson or Nokia. Ironically, the most prominent OpenRAN solution, the ORAN Alliance, has a strong Chinese presence and includes contributors that have been sanctioned by the Biden administration. Hence, we suggest the careful promotion of OpenRAN solutions. EU and European companies are investing in OpenRAN approaches and may not be taking due care of the security risks involved. At this stage, we do not consider the ORAN Alliance to be trustworthy enough for the EU.[97]

Preserving political capability: strengthening European strongholds

Apart from technical network security risks, technological overdependencies have been identified as strategic choke points that could affect the EU's capacity for autonomous foreign policymaking. Wireless infrastructure technology is an ecosystem that has the interdependencies of a highly diversified supply chain. In isolation, individual EU member states, for example, are overly dependent on non-European suppliers of semiconductors.[98] In its entirety, however, there are strong expertise centres for the design of new wireless infrastructure based in Europe, Ericsson and Nokia being prime examples. Innovative design is a key strength of the EU. China has tried hard to create a more "entrepreneurial" climate and greater creative thinking, but this has not yet resulted in innovation quality comparable to that in the EU and the US. Asian and North American countries profit from R&D based in the EU. It is questionable, however, whether Huawei is strategically dependent on European innovation, but ASML at least remains a choke point as a semiconductor vendor of the utmost strategic

[96] Jan-Peter Kleinhans, *Whom to Trust in a 5G World? Policy recommendations for Europe's 5G challenge*, Berlin, Stiftung Neue Verantwortung, 2019.

[97] See Jan-Peter Kleinhans' and Tim Rühlig's forthcoming CHERN Policy Brief on the ORAN alliance.

[98] Jan-Peter Kleinhans (2021): The lack of semiconductor manufacturing in Europe Why the 2nm fab is a bad investment. Berlin: Stiftung Neue Verantwortung.

importance. Only collaborative action can support the EU's role on the global stage.

Acknowledging the need for collaboration in a geopolitical context, the EU is aiming for "open strategic autonomy" and has identified the need to invest in the technology required for wireless infrastructure in the 2030 Digital Compass. However, the plan aims to tackle the EU's weaknesses rather than protect its strengths. This ignores the fact that the supply chain for wireless infrastructure will remain fractured. In the field of semiconductors, for example, the EU should not aim for the unrealistic target of becoming more independent of global supply chains, but instead strengthen its position in a system of mutual interdependencies.

The need to act in unison has also led the EU to develop a 5G toolbox to facilitate a coordinated approach that addresses not only technological but also political considerations. However, member states are implementing the legally non-binding toolbox very differently.

On the issue of Huawei, for example, Sweden, at one extreme, has decided to issue an outright ban on Chinese technology in its rollout of critical components of the 5G network,[99] while, at the other extreme, Hungary remains open to Chinese 5G technology.[100] In between, EU member states have adopted a range of different regulations. Italy[101] and France,[102] for example, have passed new legislation that gives veto power not just to technological agencies, but also to the offices of their heads of government.

This lack of unity complicates the situation for the EU in a geopolitical environment of technology competition between the US and China. Only by acting in unison will the EU be able to set an effective unitary regulatory environment, and tackle the strategic dependencies and choke points mentioned above.

---

[99] PTS, "Four Companies Approved for Participation in the 3.5 GHz and 2.3 GHz Auctions," *PTS*, accessed 29 March 2021, at https://www.pts.se/en/news/press-releases/2020/four-companies-approved-for-participation-in-the-3.5-ghz-and-2.3-ghz-auctions/.

[100] Gergely Szakacs and Krisztina Than, "Hungarian minister opens door to Huawei for 5G network rollout," *Reuters*, accessed 30 March 2021, at https://www.reuters.com/article/us-hungary-telecoms-huawei-idUSKBN1XF12U.

[101] Italian Government, "Golden Power," *Governo Italiano. Presidenza del Consiglio dei Ministri*, accessed 30 March 2021, at http://www.governo.it/it/dipartimenti/dip-il-coordinamento-amministrativo/dica-att-goldenpower/9296.

[102] Government of France, "Décret n° 2019-1300 du 6 décembre 2019 relatif aux modalités de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques prévue à l'article L. 34-11 du code des postes et des communications électroniques," *LegiFrance*, accessed 5 May 2021, at https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039455649/#:~:text=Copier%20le%20texte-,D%C3%A9cret%20n%C2%B0%202019%2D1300%20du%206%20d%C3%A9cembre%202019%20relatif,postes%20et%20des%20communications%20%C3%A9lectroniques; Government of France, "LOI n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles (1)," *LegiFrance*, accessed 5 May 2021, at https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038864094#:~:text=Copier%20le%20texte-,LOI%20n%C2%B0%202019%2D810%20du%201er%20ao%C3%BBt%202019%20visant,des%20r%C3%A9seaux%20radio%C3%A9lectriques%20mobiles%20(1).

Hence, our *third policy recommendation* is a unitary approach to the regulatory and investment framework coupled with a strategy that strengthens European innovation and production strongholds. It is unrealistic for the EU to strive for self-reliance. Instead of investing in those areas of semi-conductor production that are weak in Europe and building up extreme scale fabs,[103] the EU should strengthen its strongholds such as algorithmic intellectual property, architectural know-how and design. Moreover, the visions on 6G demonstrate that wireless connectivity will continue to be a crucial technology for a diverse range of applications – both professional and personal – and environments, such as industry 4.0, healthcare, residential and logistics. Dependable wireless, for example for human-robot interaction and autonomous vehicles, will require greater reliability and lower latency than is offered by 5G. It is of strategic importance that Europe continues to invest in R&D and innovation that can feed the era beyond 5G as well.

Towards systemic rivalry? Navigating EU-China cooperation

Wireless communications technologies – both infrastructure and applications – are the result of considerable international research collaboration. It is no coincidence that telecommunications are among the technologies with a particularly high share of technical standards. Global interoperability has been achieved for several generations of mobile systems, and this has clearly been a factor in their success and the high standards of mobile service experienced today. This is maintained: first, through a periodic revision of the Radio Regulations, the international treaty governing the use of the radio-frequency spectrum, undertaken through the World Radio Conferences of the ITU;[104] and, second, through standardisation of the mobile protocols in the 3GPP. Connectivity requires interoperability at its core, and consumers expect a high degree of reliability from telecommunications. Attempts to establish parallel but interoperable systems of mobile telecommunications failed in 3G.

The innovation ecosystem of wireless mobile technology is also highly transnational. For example, Nokia, which is widely considered a Finnish company, relies on R&D in wireless technologies at its US centres, such as the Bell labs, that following a series of takeovers are now part of Nokia. Chinese technology companies are not only investing in R&D facilities in the PRC, but have also taken stakes in research centres and teams of European competitors, as these have restructured in economically challenging times. Industry is also closely cooperating with universities, both within and outside of the national bases for their

[103] See the chapter on semi-conductors in this volume.

[104] https://www.itu.int/en/ITU-R/conferences/wrc/Pages/default.aspx

headquarters. Such cooperation is necessary and useful to the EU. Issues linked to the commercialisation and application of 5G and 6G wireless technology will require collaboration with both the US and the PRC. Based on the rollout of SA 5G, the PRC has promised to promote 5G applications and use cases, and is already investing in the development of 6G. Similarly, the EU has funded many projects developing 5G technologies and putting considerable effort into aligning these initiatives through the 5GPPP. It is currently seeking a joint undertaking to promote 6G.[105]

At the same time, however, research collaboration with China is being increasingly called into question across the EU. Three concerns are fuelling the discussion: First, European entities have long feared that know-how and intellectual property were being leaked to China, undermining the competitive advantage of the EU. By this stage, however, Chinese mobile technology is highly advanced, as evidenced by the increasing share of standard contributions and standard essentiality declarations of patents by Chinese actors.[106]

Second, a lack of reciprocity in access to research funding and results could provide Chinese actors with advantages. In recent years, however, concerns have grown that Chinese funding of European academic institutions could make European know-how accessible to Chinese firms rather than EU-based companies.

Third, concerns over collaboration with Chinese actors arise from their close interlinkages with the authoritarian party-state. For example, China is developing the concept of a "civil-military fusion", which will mean that civilian high-technology innovation will be increasingly coordinated with military goals and aims. Article 7 of China's National Intelligence Law requires Chinese citizens to collaborate with Chinese intelligence services on request.

These concerns are valid but cannot lead to the end of EU-China research collaboration in the context of wireless technology. Hence, our *fourth policy recommendation* is to carefully review the conditions of collaboration. Europe should continue to cooperate with China in the 3GPP and to strive for globally harmonised standards. It is crucial, however, that Europe plays a role in safeguarding its stake and avoids a situation of dominance by PRC companies. Our research demonstrates that, as of 2018, Chinese companies had already gained significant influence in the 3GPP (see figures 1–4).

[105] https://ec.europa.eu/digital-single-market/en/news/europe-puts-forward-proposal-jointundertaking-smart-networks-and-services-towards-6g

[106] Tim Pohlmann, Knut Blind, and Philipp Heß, *Studie zur Untersuchung und Analyse der Patentsituation bei der Standardisierung von 5G. Studie im Auftrag des Bundministeriums für Wirtschaft und Energie* (Berlin: IPlytics, 2020).

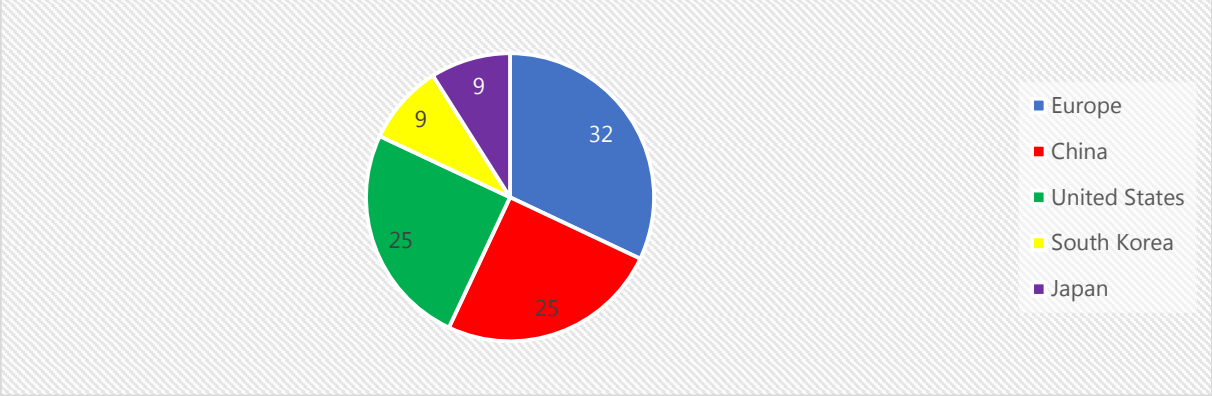

Figure 1: Votes in the 3GPP General Assembly in 2018 (in %). Source: Own graphic.

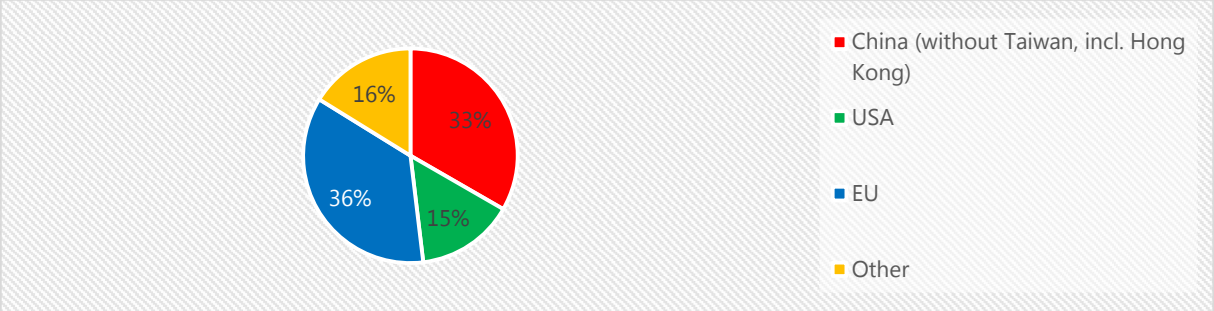

Figure 2: Submitted documents to 3GPP in 2018 (in %). Company aggregated by country of origin. Source: Own graphic.

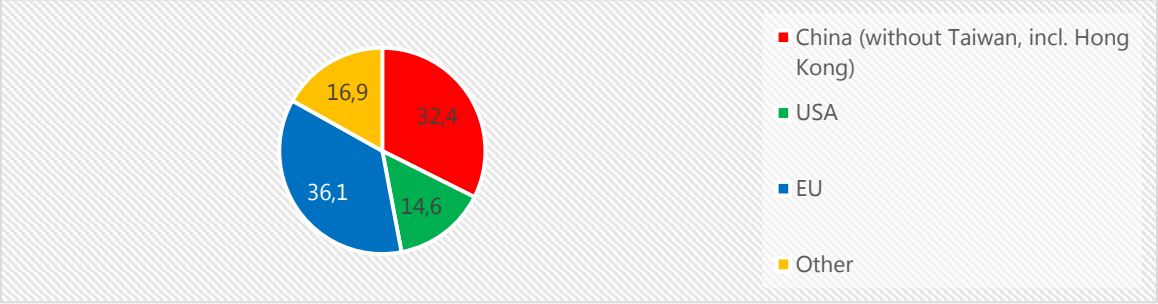

Figure 3: Accepted documents to 3GPP in 2018 (in %). Company aggregated by country of origin. Source: Own graphic.

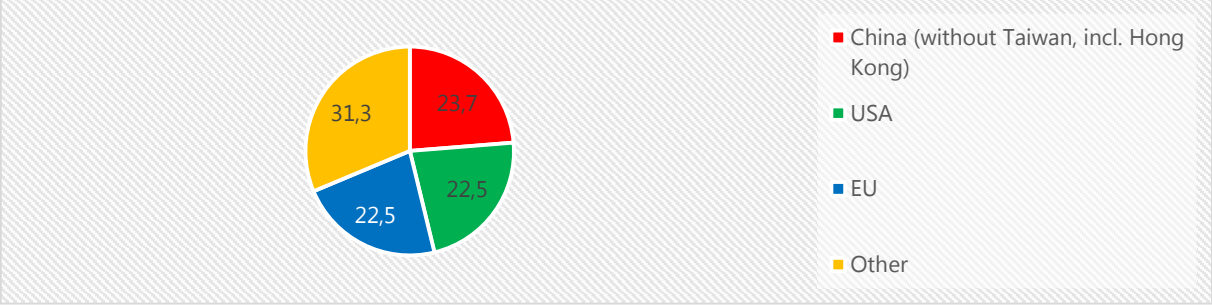

Figure 4: Participants in 3GPP standardisation in 2018 (in %). Company aggregated by country of origin. Source: Own graphic.

Conclusion: partnership, competition or systemic rivalry – what defines EU-China relations on wireless technology?

Developing an isolated European approach to future wireless networks is not an option. China will necessarily remain a partner. However, cooperation with the PRC on wireless must be subjected to careful scrutiny. This paper only clears a first path into the subject that requires much more in-depth analysis, as is the case for all four dimensions of the digital China challenge discussed above. For example, our current knowledge of China's rollout and its technical and political implications is largely limited to public pronouncements by the Chinese government.

The need for more flexible and diverse deployment requires careful consideration of the OpenRAN concept, whether to collaborate with Chinese actors in this context – and, if so, how – and the political-strategic implications for the EU.

A broader scope of study should consider Chinese involvement in wireless infrastructure built in regions such as Africa, and the strategic consequences. Technological dependencies and inherent network security vulnerabilities result in strategic dependencies that need to be properly understood for EU foreign policy to be effective.

A final example of the need for further research is a deep dive into EU-China research collaboration. While we know that Chinese scholarships and funding from Chinese technology firms play a major role, there has as yet been no comprehensive assessment of the allocation of China's financial resources to European research and its strategic implications. We do not suggest that EU-China cooperation on wireless technology should cease. However, further research would help EU policymakers to properly assess the pitfalls. We suggest that any such cooperation should be investigated under the pretext of two questions:

(1) Does cooperation with China undermine European strategic competitiveness?

This dimension largely refers to the need to maintain or achieve a strategic position in both innovation and the supply chain. This means improving the ecosystem within the EU but also preventing the overdependencies that result from cooperation with the PRC. This is where China is simultaneously a partner and a competitor.

(2) Does cooperation with China endanger network security in the EU?

Systemic rivalry largely plays out in technical network security. Wireless networks are a critical resource, and any malfunctioning will have security implications that go far beyond the networks themselves. Europe should carefully investigate the network security risks when

cooperating with China (which is not a security ally of the EU) in this field. The EU should seek to enhance the resilience of its wireless networks and cooperation needs to be subordinated to this goal.

In sum, preserving strategic autonomy requires the avoidance of overdependencies as well as the preservation of the network security of strategic wireless networks in the EU.

Authors:
Liesbet van der Perre is a Professor in the DRAM CO lab of the Electrical Engineering Department of the KU Leuven in Belgium. Contact: liesbet.vanderperre@kuleuven.be
Tim Rühlig is a Research Fellow at the German Council on Foreign Relation and an Associate Research Fellow of the Swedish Institution of International Affairs' Europe program. He is based in Germany. Contact: ruehlig@dgap.org


DPC

AI and IoT Developments in China and the Relevance for EU Policy – a scoping study

Carlo Fischione, Sanne van der Lugt, Frans-Paul van der Putten

Abstract

The risk of one-sided dependencies is greater with respect to the IoT than AI, as China has a competitive advantage in the former, the authors argue in this chapter. If the EU sticks to its principle of open markets even though European companies find it difficult to compete with China in the arena of the more advanced technologies, the EU risks to losing these companies and the Chinese government could leverage the dependency created for its political aims.

Introduction: How are China's efforts to develop Artificial Intelligence/Internet of Things capacities related to EU policy?

Aim of the scoping study.

This scoping study provides a preliminary indication of whether – and, if so, how – the efforts of the Chinese government to develop Artificial Intelligence (AI) and Internet of Things (IoT) capacities might constitute a "digital China challenge" to the EU in four distinct areas:

- The economic: do they threaten EU competitiveness?
- The political: do they enable China to leverage technological dependencies for political aims?
- Security-related: do they create vulnerabilities for the EU linked to espionage and/or sabotage?
- Ideational: do they weaken the EU's ability to protect the personal data of its citizens?

These questions should be seen against the backdrop of the changing relationship between the EU and China. The political dimension of EU-Chinese relations is becoming increasingly tense – a change linked to the overall increase in geopolitical tensions between the US and its western partners, on the one hand, and China, on the other. At the same time, advanced technologies are

increasingly regarded as crucial not only for economic competitiveness and national security, but also for the projection/protection of values and geopolitical positioning. Assessing the extent to which China-related developments in AI and IoT capacities constitute a challenge is important because it helps the EU address these challenges. The question also helps put any challenge into perspective. It is therefore also important to evaluate potential benefits, and to compare the challenges that result from developments in AI and IoT with other digital challenges – both China- and non-China-related.

Artificial Intelligence and the Internet of Things.

Artificial Intelligence refers to a set of methods and algorithms that can be implemented by software to perform operations. Examples are data analysis and automatic decision making to control software, electronic systems or any form of infrastructure where automatic decision making is needed. The Internet of Things refers to the information and communications methods, algorithms and software, and physical infrastructure that allow devices to be connected to cloud servers or internet access points, often through wireless communications.

In other words, the IoT is a set of technologies, whereas AI is a technology. The IoT is essentially a complex infrastructure, whereas AI is essentially software that can run within units of the infrastructure. It is much more complex to set up and use an IoT infrastructure than to set up and use AI algorithms. If the IoT were a car, AI would be a small software component of that car. It is much more difficult to assemble and run a car than to install and run a small component of a car. Nonetheless, a small component can have major impacts on the functioning of the car.

While the IoT deals with devices that interact using the internet, AI allows the devices to learn from their data and experience. Combining AI and IoT creates intelligent machines that simulate smart behaviour and support decision making with little or no human interference.

Recent China policies on Artificial Intelligence and the Internet of Things

New Generation Artificial Intelligence Development Plan.

Even before the launch of the New Generation Artificial Intelligence Development Plan (AIDP) in July 2017, AI had already been mentioned in China's Three-year Guidance for Internet Plus Artificial Intelligence Plan (2016–2018). The aim of the latter, which was published in May 2016, was to create a US$ 15 billion market by 2018 by investing in research and supporting the development of the Chinese AI industry.[107] It was

[107] OECD Policy Observatory, https://www.oecd.ai/dashboards/policy-initiatives/2019-data-policyInitiatives-24471

formulated jointly by the National Development and Reform Commission, the Ministry of Science and Technology, the Ministry of Industry and Information Technology and the Cyberspace Administration of China.[108] In May 2017, the Ministry of Science and Technology announced the decision to add "AI 2.0" to the initial line-up of a series of 15 "Science and Technology Innovation 2030 Megaprojects" as a 16th megaproject.[109]

Although the stated intention of these previous policy initiatives was to develop AI, their efforts were fragmented and viewed AI as one of many tools for achieving a particular goal. In contrast, the AIDP is the first national-level legislative effort to focus explicitly on the development of AI as a unified strategy. The AIDP sets out China's long-term perspective on AI and sets industrial goals for each period. These comprise:

1) By 2020, the Chinese government aims to keep pace with all leading AI technology and its general application. In monetary terms, the Chinese government intends to create an AI industry worth more than 150 billion yuan (c. €19 billion). In terms of ethics and regulation, it is seeking to establish initial ethical norms, policies and regulations on vital areas of AI. These goals have not been properly operationalised, however, and COVID-19 measures have made it difficult for foreign researchers to access the country to evaluate whether the Chinese government has achieved them. Nonetheless, it is estimated that the value of the Chinese AI fundamental technology market was almost 50 billion yuan in 2020.[110]

2) By 2025, the Chinese government aims to have achieved major breakthroughs in basic AI theory and to be world-leading in some applications. It is also targeting an increase in the value of China's core AI industry to over 400 billion yuan (c. €51 billion), and plans to expand on and codify ethical standards for AI.

3) By 2030, the Chinese government aims to have established China as the global innovation centre for AI. By then, core AI industry growth is expected to have more than doubled again, and the AI industry to be valued at 1 trillion yuan (c. €130 billion). There will also have been further upgrades to laws and standards to deal with newly emerging challenges.

China has a number of advantages over other leading countries. China's tech giants are proactive AI researchers, patent applications are on the increase,[111] and

[108] OECD Library, AI policies and initiatives, https://www.oecd-ilibrary.org/sites/cf3f3be0-en/index.html?itemId=/content/component/cf3f3be0-en

[109] Elsa Kania, "China's AI agenda advances: As China throws state support behind AI development, major Chinese technology companies will remain integral players", *The Diplomat,* 14 February 2018, https://thediplomat.com/2018/02/chinas-ai-agenda-advances/

[110] Daniel Slotta, "Size of the AI basic technology market in China 2019–2025", Statistica, 18 August 2021, https://www.statista.com/statistics/1257417/china-ai-fundamental-technology-market-size/

[111] Although we need to be careful about lumping all patent applications together, since the essentiality of patents is not always the same. More in-depth research will be needed in order to be able to say

there is a huge potential market. However, despite the efforts the Chinese government is putting in to promote higher education in AI technology,[112] the biggest challenge for Chinese firms remains the lack of skilled engineers with the required AI grounding (see Figure 1).

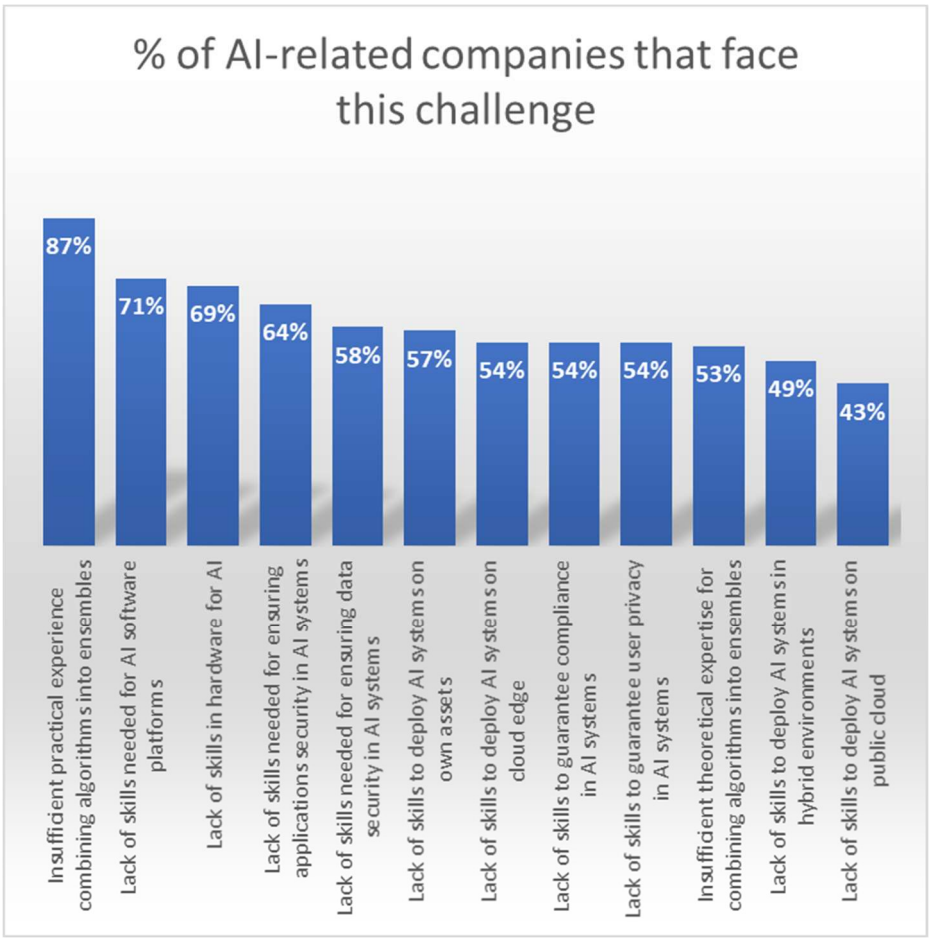

Figure 1. Overview of the challenges facing Chinese AI-related companies Source: Forrester Consulting, Industrial AI Development White Paper, 2018.

Publication of the AIDP was followed by an AI-related state conference in November 2017. This established: (a) a New Generation Artificial Intelligence 2030 Innovation Megaproject; (b) a New Generation AI Promotion Office, formed by contributions from 15 different governmental/ Chinese Communist Party bodies; (c) a New Generation AI Strategic Advisory Committee, a list of members of which is published online; and (d) the first batch of National AI Open Innovation Platforms. The conference also highlighted that the role of

more about the essentiality of Chinese AI applications.

[112] Sarah Dai, "AI is the fastest expanding discipline in China's universities, with 180 more approved to offer it as a major", *South China Morning Post*, 4 March 2020, https://www.scmp.com/tech/policy/article/3064956/ai-fastest-expanding-discipline-chinas-universities-180-more-approved

enterprises should be strengthened, and that international cooperation on R&D on AI technologies should be deepened.[113]

14th Five-year Plan on AI and the IoT, 2021–2025[114]

The 14th Five-year Plan (FYP) for the period 2021–2025 was formally adopted on 11 March 2021. A major aim of the plan is to strengthen China's technological self-reliance.[115] One method for achieving this aim is to promote closer collaboration between academia and industry in China.[116] AI is one of the technological focus areas of the FYP and is mentioned several times in four different chapters.[117]

Chapter 2 on innovation-driven development:

- Integrate and optimise the allocation of scientific and technological resources to AI (among other domains).
- Strengthen original and leading scientific and technological research on AI (among other domains).

Chapter 5 on the digital economy and building a digital China:

- Strengthen the innovative application of key digital technologies, one of which is AI.
- Accelerate the promotion of digital industrialisation in AI (among other domains).
- Strengthen network security protection by accelerating innovation in artificial intelligence security technologies

Chapter 13 on citizens' (国民) suzhi/quality (素质) and all-round development of the people (人)

- AI is an area for education-industry integration with the aim of improving educational quality.

Chapter 16 on the military:

- Promote the simultaneous improvement of national defence

[113] 科技部召开新一代人工智能发展规划暨重大科技项目启动会 [The Ministry of Science and Technology held a new generation of artificial intelligence development plan and major science and technology project launch meeting], Cyberspace Administration of China, 16 November 2017, http://www.cac.gov.cn/2017-11/16/c_1121964697.htm

[114] Research for this section was conducted by Vera Kranenburg during her internship at the Clingendael China Centre.

[115] It should be noted that China has long been dependent on western technology in crucial sectors such as telecom infrastructure (routers from CISCO, digital switches from Bell Telephone Manufacturing Company), navigation system (GPS) and international financial transactions (SWIFT), among other things. While the US government focuses on its trade deficit with China, the Chinese government worries about the IP deficit. In the past 20 years, Huawei alone paid more than $6 billion in fees and royalties, of which almost 80% went to US companies.

[116] Smriti Mallapaty, "China's five-year plan focuses on scientific self-reliance", *Nature*, 11 March 2021, https://www.nature.com/articles/d41586-021-00638-3

[117] 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 [Het 14e vijfjarenplan voor nationale economische en sociale ontwikkeling van de Volksrepubliek China en een voorlopige visie voor 2035], *Xinhuanet*, 12 March 2021, http://www.xinhuanet.com/2021-03/13/c_1127205564.htm

strength and economic strength, through deepened military-civilian scientific and technological collaboration on innovation, and strengthened military-civilian coordinated development in AI (among other domains).

The Internet of Things is mentioned seven times in the FYP, in two different chapters.

Chapter 3 on industry and the development of the real economy:

- Promote the all-round development of the Internet of Things, and create IoT access capabilities that support fixed-mobile convergence and the combination of broadband and narrowband.

Chapter 5 on building a digital China:

- Promote the construction of new smart cities, incorporate IoT sensing facilities and communication systems into the unified planning and construction of public infrastructure, and promote the application and intelligent transformation of the Internet of Things in municipal public facilities and buildings.

In sum, rapid advances in technology is a major goal of the FYP, and both AI and the IoT are regarded as highly relevant technological domains by the Chinese government.

Current developments: Evidence from the ground

Short overview of the current state of AI and IoT technology in China.

This section provides a short overview of the current state of AI and IoT technologies in China. We have reviewed articles linked to reputable conferences and to journals published by Chinese institutions in the period 1975–2021, as tracked by Web of Science. In particular, we searched Web of Science using the keywords "Internet of Things" and "IoT", as well as "Artificial Intelligence" and "AI" and "Machine Learning". The number of articles presented at technical conferences and published by journals provides an indication of the ability to innovate in the AI and IoT domains, and of the number of researchers pushing the development of AI and IoT. However, the number of publications does not tell us the precise real-world implications of these published articles.

Artificial Intelligence.

Figure 2 is an international comparison of AI articles and the patents cited in academic papers published by reputable journals or presented at conferences. The Web of Science only considers publications by reputable journals or papers presented at reputable conferences, and the patents are only those cited in these publications. This is a reasonable initial survey, since a patent itself may be of low value even if it is cited in other

patents. China had 11605 publications and academically cited patents, which made it the second-largest contributor after the US, which had 15091.

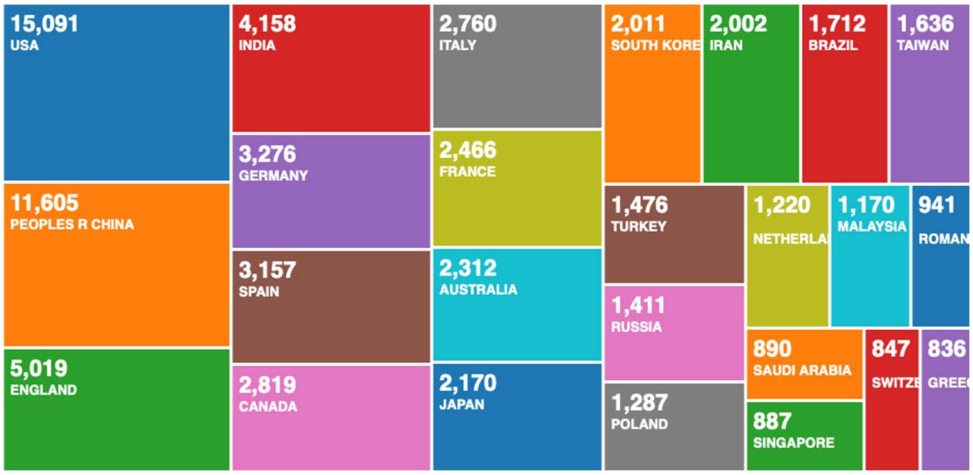

Figure 2: AI publications and academic-cited patents, 1975–2021 Source: created by the authors based on data from Web of Science

Figure 3 shows the number of AI publications per year in China. There has been a sharp increase since 2019, when the number of publications per year almost doubled.

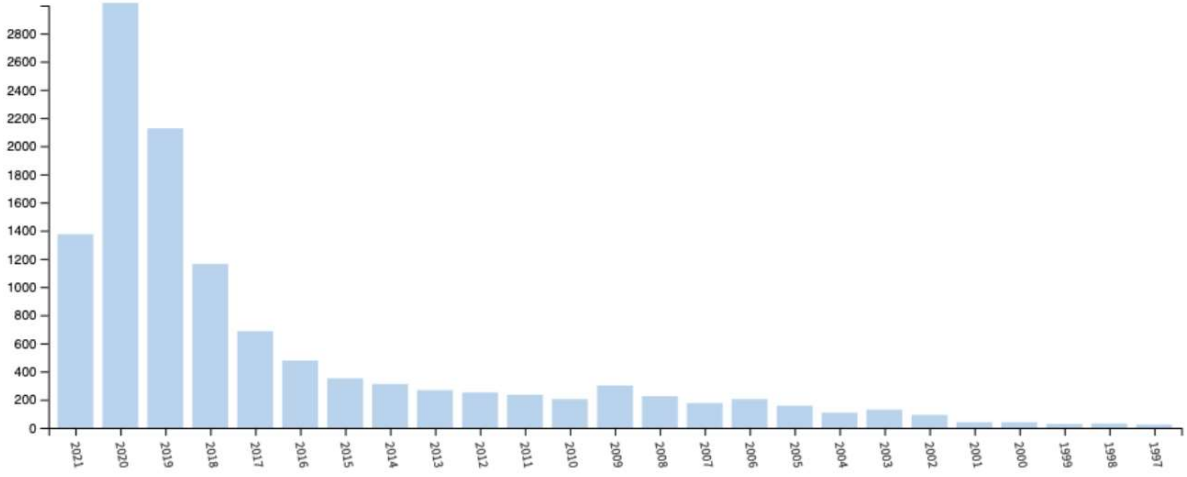

Figure 3: AI publications and academic-cited patents in China, 1997 to mid-2021. Source: created by the authors based on data from Web of Science.

For comparison, Figure 4 shows the number of AI publications per year in Europe. The rate of increase in European AI publications is similar to China. The main difference, however, is that the number of AI publications in Europe is one order of magnitude greater than in China. This raises the question of why China is lagging behind in terms of AI publications and academic-cited patents. Is the west too advanced for China to catch-up? Or is it just a matter of time? Does the Chinese government have other political priorities? Future research should look more deeply into these questions.

One of the main reasons why China is lagging behind is that its research on AI is mostly at lower Technological Readiness Levels (TRL), where a past history of research is important in spurring and triggering new research results. To create fundamentally new research ideas at low TRLs, it is essential to live on the wave of a long research history that pushes ground-breaking original ideas on top of past ideas. It is arguable that China has a shorter history of research at lower TRLs, especially when it comes to more mathematically oriented questions and the mathematical foundations of AI. It is probably only a matter of time, however, before China is able to develop and create a sufficiently long research tradition and large volume of results in the AI field to be able to compete with Europe.

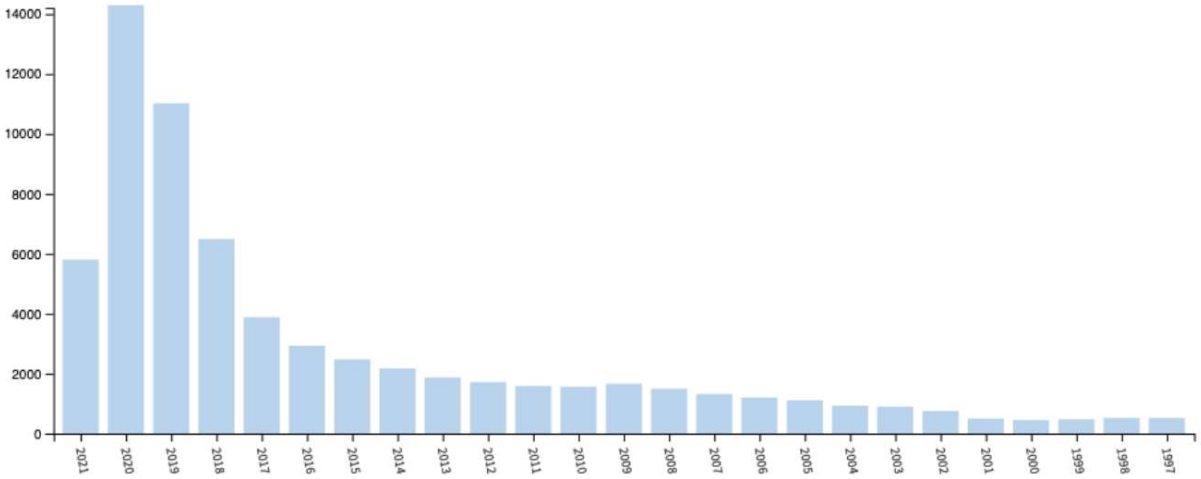

Figure 4: AI publications and academic-cited patents per year in Europe, 1997 to mid-2021. Source: created by the authors based on data from Web of Science

Internet of Things

Figure 5 shows the number of IoT-related publications per country. It shows that China dominates the IoT area with 7960 publications, compared to just 1212 in the US in the same period and 1044 publications from Europe.

Figure 5 Global IoT publications and academic-cited patents, 1975 to mid-2021. Source: created by the authors based on data from Web of Science.

Figure 6 shows the number of IoT publications and academic-cited patents per year in Europe since 2002. The rate of increase is modest, and the total number of IoT-related publications and academic-cited patents is almost an order of magnitude smaller than China's. This raises the question of why China is so much more advanced in IoT publications than the EU. Does China have a better ecosystem? Is China profiting from being a latecomer able to direct its resources more quickly to the most innovative areas? Is this a political choice? One explanation might be that Chinese researchers and engineers are able to assemble IoT systems by reading publications on the individual components and technologies of IoT due to China's TRL for IoT, which is generally higher than for AI. To produce lower TRL results requires greater originality in order to introduce new concepts or ideas. Such originality is often based on a longer research history, which provides the basis for and insights required to generate new ideas and concepts. A high level of originality also requires freedom to perform blue skies research, which will have an impact several decades after the new ideas are generated. IoT is at a higher TRL because it is a composition of several technologies, and thus requires fewer original ingredients. At a higher TRL, novelty and impact are generated by the composition of ideas and ingredients that already exist on their own. Thus, IoT systems come to the market much earlier than low TRL ideas and systems. That said, future research should look into this more deeply.

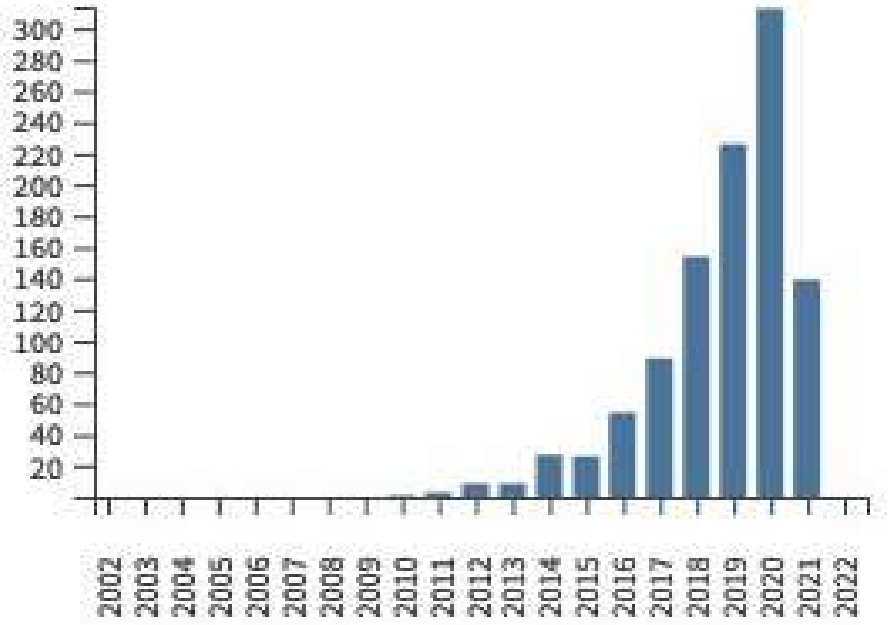

Figure 6: IoT publications and academic-cited patents in Europe, 2002–2020. Source: created by the authors based on data from Web of Science

Figures 7 and 8 show the impact of IoT publications from Europe and China, respectively. Although China has almost an order of magnitude more publications than Europe, the Chinese IoT publications have only 50% more impact than European IoT publications.

Figure 7: Impact of IoT publications and academic-cited patents in Europe, 1975–2020. Source: created by the authors based on data from Web of Science

Figure 8: Impact of IoT publications and academic-cited patents in China, 1975–2020. Source: created by the authors based on data from Web of Science.

In this brief overview, we have observed that Europe dominates China with regard to the number of academic publications on AI, but the trend is reversed with the IoT. As is explained in the introduction, it is more difficult to develop IoT technology than AI technology because the IoT is a collection of software and hardware infrastructures, whereas AI is an algorithm that can be implemented as part of software or hardware infrastructure.

However, more research is needed to distinguish between articles presented at conferences or published by journals, and patents. Future research should also incorporate a more detailed patent analysis that includes forward citations. In particular, the current analysis has not considered patents that are not cited in academic papers. A deeper analysis would have to investigate the total amount of patents and their citations, in both other patents and reputable academic venues. To do so, several databases for patents and academic publications would have to be consulted, cross-correlated, and cured, as patent databases do not report academic publication, whereas high-quality academic publications only report articles presented in reputable venues and citations of patents from those reputable academic articles. We also need to extend the research to those keywords closely related to AI and IoT, and that constitute the same methodological or technological domain, such as "wireless sensor networks" or "machine to machine communications". It will also be interesting and useful to ascertain in which engineering and societal domains AI and IoT are being used predominantly. Moreover, the publications mostly discuss research efforts at low TRLs, whereas the commercial and industrial impact is more evident from research at TRLs 7–9.

Case study: industrial cleaning robots

To illustrate the relevance of AI and the IoT to the EU in concrete terms, this section presents a case study on industrial cleaning robots. COVID-19 has accelerated the need for robots, and specifically for those with a cleaning function. Robots have taken over the physically intense tasks of cleaners on an increasing number of factory floors and offices, to allow a human focus on the more specialised cleaning tasks. All the major industrial cleaner suppliers in the Netherlands are currently either offering or developing a robotic cleaning vehicle.

A cleaning robot can be very convenient, but it also has the potential to become highly inconvenient if this robot begins collecting and sharing data that is not supposed to be shared. What data can an autonomous cleaning robot collect? What are the possible security risks associated with the use of such a robot?

A cleaning robot uses exteroceptive sensors – such as lasers, distance sensors

and cameras – to create a floor map, locate itself, avoid objects and stairwells, recognise glass walls and communicate with lifts. Depending on the type of camera the robot uses, it could make detailed records of its surroundings and the people walking around. This could include sensitive, personal and/or secret information. Some manufacturers therefore consciously choose not to place cameras on the robot and instead use only lasers (LiDAR sensors) and ultrasonic sensors.

Data leaves the robot, and the cleaning location, to be converted into information. Moving and storing this information can present security risks if the data contains privacy-sensitive or classified information. It appears that data collected by non-European brands is being stored outside Europe.[118]

Table 1 lists the three European brands currently actively operating on the Dutch market, two of which use their own software. This means that Adlatus and Cleanfix are the only industrial cleaning robots on the Dutch market that do not store data outside of Europe.

Name of Company	**HQ**	**Software**	**Number of models**
Tennant	US	BrainOS	2
Hako	US	BrainOS	3
ICE Robotics/ Softbank	China/Japan	BrainOS	1 (soon to be 4)
Nilfisk	Denmark	BrainOS	2
Cleanfix	Switzerland	Own software	1
Adlatus	Germany	Own software	1
Gaussian Robotics	China	Own software	3 (soon to be 6)

Table 1. Supply of industrial cleaning robots on the Dutch market. Source: Compiled from interviews with suppliers of industrial cleaning devices in the Netherlands

European models can expect fierce competition from China's Gaussian Robotics. Founded in 2013, the company employs approximately 450 people, around 250 of whom are engineers. Gaussian Robotics is the market leader in intelligent cleaning robots in China. A recent joint KPMG/Clingendael report on industrial cleaning robots[119] shows that the Gaussian robot is more advanced in terms of autonomous problem-solving than most – if not all [120]– European and US brands on the Dutch market. The US brands, for example, stop and call the operator when someone or something is in their pre-programmed way, while the

[118] Sanne van der Lugt and Marnix Bel, "How smart is the use of smart devices in the office? The case of industrial cleaning robots in the Netherlands", Clingendael Report, April 2021, https://www.clingendael.org/sites/default/files/2021-04/Report_Smart_devices_office_industrial_cleaning_April_2021.pdf

[119] van der Lugt and Bel (note 118).

[120] Perhaps with the exception of the European brand Fybots, although the researchers did not receive enough information from Fybots to make a fair comparison.

Gaussian robots first wait to see whether the obstacle is moving and then wait for the obstacle to get out of the way. If the obstacle does not move, a Gaussian robot tries to go around it. If there is no space, it will go back and change its route to see if it can approach the same place from another direction. Some European brands should theoretically be able to do this, but in reality it is still too difficult for them. Gaussian's advantage is probably the number of robotic engineers it has compared to its European competitors. Its more advanced technology makes the Gaussian robot an attractive option for European customers.

If customers and companies choose advanced Chinese cleaning robots over European brands, the market share of European companies will decline. If Gaussian also opts to increase its market share in Europe using a pricing strategy – in a similar way to how Huawei and ZTE entered the European market for telecoms[121]– this could lead Gaussian's competitors to throw in the towel one by one. Customers for industrial cleaning robots will then be left with no choice but a Chinese robot and less control over their data.

Recent EU policies on AI and the IoT: Are EU policies fit for China's rise?

The EU 2030 Digital Compass.

On 9 March 2021, the European Commission presented a vision of and avenues for Europe's digital transformation by 2030. This vision for the EU's digital decade evolves around four cardinal points (see Figure 9).

[121] In a similar way that Chinese telecom vendors Huawei and ZTE pushed Western vendors out of the market using a price war, which is the reason why there are globally only four telecom vendors left: two Chinese (Huawei and ZTE) and two European (Ericsson and Nokia Alcatel-Lucent). See "EU-china investments: The 5g political power game", Clingendael Institute, 25 February 2019, https://spectator.clingendael.org/nl/publicatie/eu-china-investments-5g-political-power-game. Ericsson and Nokia barely survived the price war with Huawei but are currently benefiting from the trade war between the US and China.

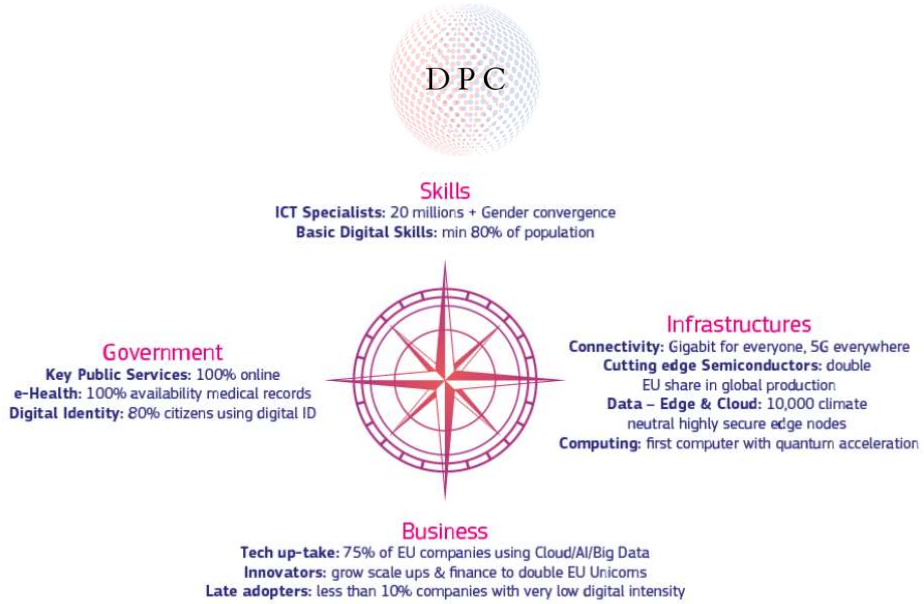

Figure 9 Digital Compass. Source: European Commission, 2030 Digital Compass: The European way for the digital decade*, 2021.*

The EU's aim is to be digitally sovereign in an interconnected world and to turn Europe into the global hub for trustworthy AI. However, the Commission's claim that it had established "the first-ever legal framework on AI"[122] is incorrect because the Chinese government launched its cybersecurity law in July 2017.[123] Whereas Chinese regulation focuses only on providers, however, the EU's AI regulation is broader and applies to providers, importers, distributors and operators/users.[124]

AI does not have the central role in the EU's digitalisation strategy that it has in China's. AI is mentioned as just one of a number of crucial technologies, such as 5G, the IoT, edge computing, robotics and augmented reality, that will be at the core of new products, new manufacturing processes and new business models. Nonetheless, in April 2018 the Commission adopted a coordinated plan for AI. The plan recognises that there is a lack of capacity in the EU in terms of specialised education and training programmes on AI, and that massive investment will be required to train future generations of workers and to upskill and reskill the workforce.

The Commission has called for swift adoption and implementation of its proposals on the Digital Single Market. However, the question arises whether action will be quick enough for the EU to become digitally sovereign. The Commission expects to be able to make a difference in "ethical" AI and is seeking to build on a renewed transatlantic relationship and a wider coalition of like-

[122] European Commission, Shaping Europe's DigitalFuture, "Digital Economy and Society Index 2021: overall progress in digital transition but need for new EU-wide efforts" [n.d.], https://digital-strategy.ec.europa.eu/en

[123] Guanghao Zou and Hong Zhang, "Future of IP: China, a closer look at governmental and regulatory support of AI", Managing IP, 3 March 2021, https://www.managingip.com/article/b1qsl1ghs6s37w/future-of-ip-china-a-closer-look-at-governmental-and-regulatory-support-of-ai

[124] Lexology, "EU announces first ever legal framework for regulating artificial intelligence", 19 May 2021, https://www.lexology.com/library/detail.aspx?g=1489818a-760f-404c-8fea-e2aa863d235e

minded partners that share its vision of a human-centric digital transformation. The purpose of this proposed coalition is to defend "the open, decentralised internet, based on a single worldwide web, and a use of technology that respects individual freedoms and promotes a digital level playing field". Table 2 lists the European Commission's digital ambitions for 2030.

EU's objective for 2030: "The continent with a high share of digitalised businesses"		
Dimension	**2030 EU Target vs baseline**	**Source**
Take up of digital technologies	**75% of European enterprises** have taken up: - Cloud computing services (2020 baseline: 26%) - Big data (2020 baseline: 14%) - Artificial Intelligence (AI) (2020 baseline 25%)	ESTAT, IPSOS
Digital "late adopters"	**More than 90% of European SMEs** reach at least a basic level of digital intensity[9] (2019 baseline : 60.6%)	DII, ESTAT
Innovative businesses/scale-ups	Europe will grow the pipeline of its innovative scale ups and improve their access to finance, leading to **doubling the number of unicorns**[10] (2021 baseline: 122)	Dealroom (used by Atomico in its state of European tech)

Table 2: Overview the EU's digital objectives for 2030. Source: European Commission, 2030 Digital Compass: The European way for the digital decade*, 2021*

The 2018 Coordinated Plan on AI.

The 2018 Coordinated Plan on AI represents a joint commitment by the European Commission and the EU member states to work together to maximise Europe's potential to compete globally. It lays the groundwork for cooperation, defines areas for investment and encourages member states to develop national strategic visions on AI. As a result of the actions agreed and facilitated by the 2018 Coordinated Plan, most member states have adopted national AI strategies and begun to implement them. Investments in AI have increased and the EU has been able to mobilise a critical resource pool to support these processes.

A review of the Coordinated Plan in 2019 proposed a concrete set of joint actions for the European Commission and the member states to create EU global leadership on trustworthy AI. The proposed key actions reflect the vision that to succeed, the EU needs to:

- accelerate investments in AI technologies to drive resilient economic and social recovery facilitated by the uptake of new digital solutions;
- act on AI strategies and programmes by implementing them fully and promptly to ensure that the EU reaps the full benefits of first-mover / early adopter advantages; and
- align AI policy to remove fragmentation and address global challenges.

The 2020 White Paper on AI and the Data Strategy.

Based on the 2018 Coordinated Plan on AI, the 2020 White Paper is a complex document that analyses the strengths and weaknesses of and opportunities for Europe in the global market for AI. The purpose is to set out policy options on how to create a single market for data that would maintain Europe's global competitiveness and data sovereignty. Common European data spaces should ensure that more data becomes available for use in the economy and society while keeping the companies and individuals that generate this data under control.[125]

For this to happen, a solution needs to be found to the impasse between the European General Data Protection Regulations (GDPR), which protect data stored on European territory, and the US CLOUD Act, which can force US companies to share the data they have stored abroad with the US government. Ignoring this impasse and allowing the US government access to data stored by US companies on European soil would create a precedent for other non-European companies.

The 2019 EU-China Strategic Outlook.

The 2019 EU-China Strategic Outlook describes China, in different policy areas, as:

- a cooperation partner with which the EU has closely aligned objectives,
- a negotiating partner with which the EU needs to find a balance of interests,
- an economic competitor in the pursuit of technological leadership, and
- a systemic rival promoting alternative models of governance.

The tools and modalities for EU engagement with China should therefore be differentiated depending on the issues and policies at stake. The EU should also use linkages across different policy areas and sectors to exert more leverage in pursuit of its objectives.

The Strategic Outlook concludes that the EU's response should be based on clearly defined interests and principles – the EU should deepen its engagement with China to promote common interests at the global level and a robust search for more balanced and reciprocal conditions for governing the economic relationship. Finally, to maintain its prosperity, values and social model in the long term, there are areas where the EU itself will need to adapt to changing economic realities and strengthen its own domestic policies and industrial base.

The Commission recognises that neither the EU nor any of its member states can effectively achieve their aims with regard to China without full unity. It emphasises

[125] European Commission, Shaping Europe's Digital Future, "A European Strategy for data" [n.d.], https://digital-strategy.ec.europa.eu/en/policies/strategy-data

the responsibility on all member states when cooperating with China – both individually and within sub-regional cooperation frameworks such as the 16+1 format – to ensure consistency with EU law, rules and policies.

Conclusions and recommendations for a better fit of EU policy

This section shares some preliminary insights concerning the four areas of concern mentioned in the introduction.

Do the efforts of the Chinese government to enhance national AI and IoT capacities threaten EU competitiveness?

Chinese policy and plans are focused on rapid advances in both AI and the IoT. Europe is ahead of China on AI (in terms of the number of publications and academically cited patents) but the pattern is reversed with the IoT. This means that the EU could benefit more from cooperation with China on the IoT than on AI. China's AI companies and researchers generally have more favourable access to data sets, which could constitute an advantage and speed research innovation on AI. However, this could arguably take several years due to the need for China to strengthen its fundamental research in general and AI research in particular, which is the only way to generate competitive original AI methods. The case study on industrial cleaning robots shows that the European open market is not just a strength (as noted in the Digital Compass), but also potentially problematic if European firms are confronted with more advanced technologies from outside of Europe.

Do these efforts enable China to leverage technological dependencies for political ends?

The risk of one-sided dependencies is greater with regard to the IoT than AI, as China has a competitive advantage in the former. However, this will also depend on the EU's response to developments in China. If the EU sticks to its principle of open markets even though European companies have difficulties competing with more advanced technologies from China, it risks losing these companies, and the Chinese government could leverage the created dependency for political ends.

Do they create vulnerabilities for the EU concerning espionage and/or sabotage?

The case study on industrial cleaning robots shows that continuing to rely on market forces and to leave European companies to their fate could create vulnerabilities to espionage and sabotage.

Do they weaken the EU's ability to protect the personal data of its citizens?

The case study on industrial cleaning robots shows that it is not necessarily potential dependency on China for crucial technology that weakens the EU's ability to protect the personal data of its citizens as much as the impasse between the European GDPR and the US CLOUD

Act. Once the EU has resolved this impasse with the US and regained sovereignty over all the data stored on European soil, it will be able to force all non-European firms to store the data they collect in Europe.

It is too early to present policy recommendations based on this highly preliminary study. However, it is possible to conclude that the four-dimensional threat analysis seems promising and should be explored more thoroughly. We recommend including an assessment of the potential benefits to the EU and a comparison with other Chinese and non-Chinese digital challenges.

The cleaning robot case study shows us that China is already ahead of Europe in some areas. Consideration should therefore be given to whether it is easier to impose restrictions on non-European companies entering the European market than to accomplish full reciprocity in terms of increased access to the Chinese market to achieve the degree of openness that the EU market currently provides. We need to understand better that the main motivation behind the focus on technological development in China is for China to become self-reliant. China is moving away from a situation in which it was overly dependent on Western technology and intends never to return to that level of dependency. For this reason, it is unlikely that the Chinese government could ever be induced by the EU to substantially increase European access to the Chinese market.

The Digital Compass calls for Europe to focus on its strengths: "an open and competitive single market, strong rules embedding European values, being an assertive player in fair and rules-based international trade, its solid industrial base, highly skilled citizens and a robust civil society". However, as the case of the robot cleaners shows, an open market can become problematic when European firms are confronted with more advanced technologies from outside Europe.

This pilot study suggests that further research will be crucial to understanding more precisely where and to what extent Europe needs collaborative research and business ties with China in order to advance its capabilities in AI and the IoT, and which criteria make the difference between desirable and undesirable forms of Sino-European tech collaboration. Such research will require a joined-up approach that involves technological and China-related expertise.

Authors:
Carlo Fischione is a full Professor of Internet of Things at the KTH Royal Institute of Technology in Sweden. Contact: carlofi@kth.se
Sanne van der Lugt is a Research Fellow at the Leiden Asia Centre in the Netherlands. Contact: sannevdlugt@fastmail.com
Frans-Paul van der Putten is a Senior Research Fellow at the Clingendael Institute and Coordinator of the institute's China Centre. Contact: fputten@clingendael.org

Inflaming Transatlantic Tensions? China's Public Diplomacy Efforts to Influence EU-US Relations

Una Aleksandra Bērziņa-Čerenkova, Elena Ferrari, Julia Voo[126]

Abstract

In this initial exploration, the authors explore efforts by Chinese government representatives in the EU to influence European public opinion during the 2020 US Presidential elections. Over a four-week period around 3 November 2020, they examine the tweets of 25 Chinese government EU-based Twitter accounts to assess whether there was an enhanced and sustained effort to influence European public opinion on key geopolitical issues. Their analysis identifies Chinese government efforts on Twitter to influence European public opinion on the US, including through proxy references. Further research is required to establish the link between global Chinese government accounts and European-based Chinese government representatives, as well as to test more advanced tools for tweet retrieval, for example through sentiment analysis.

Context

Societies today are particularly vulnerable to information campaigns in the digital space. Such information campaigns range from mostly commonplace state-led public diplomacy efforts to more nefarious disinformation and misinformation efforts that have been seen in recent years. This study starts from an initial examination of Chinese government public diplomacy efforts in the European Union. The aim is to emphasise the need for continuing close examination of this topic by a multidisciplinary team of technical experts and sinologists to better understand and protect against threats to European democracy.

The public diplomacy efforts studied here are the efforts made by the Chinese Communist Party (CCP) to influence the EU institutions and EU member state governments by influencing European

[126] The authors wish to thank Son Ha Suan, a Phd student at the University of Insubria (Italy), for his help in crawling the Twitter dataset used for the preliminary analysis reported in this paper.

citizens.[127] The different forms of information manipulation range from uncoordinated efforts by non-state actors to coordinated campaigns driven by state and state-sponsored actors against several EU member states.[128] The focus of this paper is solely on public diplomacy efforts by the Chinese government, rather than disinformation or misinformation.

It is important use rigorous quantitative methods to continue to raise awareness of Chinese government efforts to influence the European public. Tackling disinformation is already a priority of the European Commission, as set out in several initiatives such as the Code of Practice on Disinformation, the European Digital Media Observatory and the European Democracy Action Plan. This analysis seeks to complement these efforts by exploring the extent to which the Chinese government has sought to influence European public opinion in the past year.

Enhancing the Chinese government's influence outside of China has become an increasingly important priority for the CCP as China's economic, trading, diplomatic and military strength have grown in parallel.[129] China's 14th Five-year Plan for the period 2021–2025 emphasises the need to focus on "presenting a positive image".[130] The CCP employs state media, and domestic and global social media platforms to disseminate public diplomacy efforts in order to influence public opinion and obscure often unhelpful truths. The objective is to "strengthen China's discourse power – or a country's power to set the agenda in the international arena by influencing the political order and values globally".[131] The CCP disinformation strategy is led by the People's Liberation Army, the State Council and the CCP United Front Work Department.[132] Recent studies have found that Beijing prioritises messaging on the strength of the People's Republic of China (PRC), its economy and its military, and contrasting this with weaknesses abroad. China's mask

[127] Public diplomacy as defined in G. D. Malone, "Managing public diplomacy", *The Washington Quarterly*. vol. 8, no. 3 (1985), pp. 199-213.

[128] European External Action Service (EEAS), "Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic: EU vs. Disinfo", EEAS Special Report Update, 24 April 2020, https://euvsdisinfo.eu/uploads/2021/04/EEAS-Special-Report-Covid-19-vaccine-related-disinformation-6.pdf.

[129] D. Roberts, "China's disinformation strategy: Its dimensions and futures", Atlantic Council, December 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/12/CHINA-ASI-Report-FINAL-1.pdf.

[130] Digital Forensic Research Lab, *Chinese Discourse Power: China's Use of Information Manipulation in Regional and Global Competition*, Atlantic Council, October 2020.

[131] Digital Forensic Research Lab, *Chinese Discourse Power: China's Use of Information Manipulation in Regional and Global Competition*, Atlantic Council, October 2020.

[132] Digital Forensic Research Lab, *Chinese Discourse Power: China's Use of Information Manipulation in Regional and Global Competition*, Atlantic Council, October 2020.

diplomacy efforts in the early months of the pandemic are a good example of this.[133]

China has a track record of using public diplomacy and disinformation campaigns to denigrate geopolitical opponents, the US in particular. Reports have highlighted how Chinese social media companies have played a key role in spreading news critical of the US electoral system while directing criticism at both former US President Donald J. Trump, and US President Joe Biden and US Vice President Kamala Harris.[134] Similarly, public security officials and diplomats in the CCP have used Facebook, Twitter and YouTube to promote China's rise.[135] "Wolf Warrior" diplomacy describes aggressive Chinese government representatives who manifest their ire in confrontational tweets while also acting as agents of public diplomacy. They have also been found to be spreading fake news and doctored images.[136]

The CCP has targeted conspiracy narratives and disinformation on COVID-19 throughout the EU and its broader neighbourhood for the past two years.[137] A primary focus of these efforts to influence European public opinion has been to curtail mentions of Wuhan as the origin of COVID-19.[138] Other studies have unearthed attempts by the CCP to use Twitter to shape the narrative around the anti-Security Law protest in Hong Kong.[139] In its analysis of CCP attempts to influence the protests in Hong Kong, Australia's Strategic Policy Institute found that the accounts associated with criticising those protests had also been active in earlier information operations targeted at political opponents of the Chinese government dating back to April 2017. Other CCP-backed influencing campaigns were targeted at foreign politicians such as the US House of Representatives Speaker, Nancy Pelosi, and the former British Foreign Secretary, Dominic Raab, often accusing them of interfering in Chinese domestic affairs.

The platforms themselves have taken steps to limit the amount of

[133] Brian Wong, "China's mask diplomacy", *The Diplomat*, 25 March 2020.

[134] Jun Mai and Guo Rui, "China may be quiet on US election but state media is drawing attention to pockets of chaos in America", *South China Morning Post*, 6 November 2020.

[135] M. Schliebs et al., "China's public diplomacy operations", Oxford Internet Institute, 11 May 2021, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/05/Chinas-Public-Diplomacy-Operations-Dem.Tech-Working-Paper-2021.1-4.pdf.

[136] Digital Forensic Research Lab,. *Chinese Discourse Power: China's Use of Information Manipulation in Regional and Global Competition*, Atlantic Council, October 2020.

[137] European External Action Service (EEAS), "Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic: EU vs. Disinfo", EEAS Special Report Update, 24 April 2020, https://euvsdisinfo.eu/uploads/2021/04/EEAS-Special-Report-Covid-19-vaccine-related-disinformation-6.pdf.

[138] Io Dodds, "China floods Facebook with undeclared Coronavirus propaganda ads blaming Trump", *Daily Telegraph*, 5 April 2020.

[139] T. Uren et al., "Tweeting through the Great Firewall", Australian Strategic Policy Institute, 19 August 2019, https://www.aspi.org.au/report/tweeting-through-great-firewall.

disinformation posted from government sponsored accounts. In 2019, for example, in an attempt to reduce the amount of disinformation and misinformation appearing on its platform, Twitter suspended more than 5,000 accounts that it suspected of being controlled by the Chinese state and released data about them.[140] However, efforts by Chinese government actors persist to influence public opinion in the EU and further afield.[141] A study by ProPublica tracked more than 10,000 suspected fake Twitter accounts with ties to the Chinese government that were involved in a coordinated influence campaign.[142] It found covert Chinese operations on Twitter criticising demonstrators at the protests in Hong Kong and spreading disinformation about the coronavirus outbreak. At the height of the epidemic, the accounts posted tweets in support of the Chinese government that called on citizens to unite against the epidemic and "dispel online rumours". These fake accounts adopted a pattern of activity that included the coordinated use of hashtags on trending topics such as COVID-19 and Hong Kong in order to gain visibility. The posts were engaged with by other fake accounts that liked and reposted them, adding positive comments presumably to boost their visibility on Twitter's algorithms. ProPublica's analysis traced these influence operations to OneSight (Beijing) Technology Ltd, a Beijing-based internet marketing company. Further digging revealed that OneSight had a contract to boost the Twitter following of the China News Service, the country's second largest state-owned news agency which operates under the United Front Works Department – an arm of the CCP responsible for influencing operations in foreign countries. While limiting the spread of disinformation is something that platforms take seriously, there is little they can do to help blunt the effect of genuine public diplomacy campaigns. An alternative approach is needed.

Our initial analysis identified persistent efforts by the Chinese government to influence European public opinion, despite the initiatives introduced by EU institutions and the social media platforms themselves. Our objective is to identify ways in which the EU and partners can limit the effectiveness of China's efforts to influence European public opinion to better protect the interests and national security of EU member states and their citizens.

[140] See "Information operations directed at Hong Kong", Twitter Safety Blog, 19 August 2019; and "Disclosing New Data to Our Archive of Information Operations", Twitter Safety Blog, 20 September 2019.

[141] See "Information operations directed at Hong Kong", Twitter Safety Blog, 19 August 2019; and "Disclosing New Data to Our Archive of Information Operations", Twitter Safety Blog, 20 September 2019.

[142] Jeff Kao and Mia Shuang Li, "How China built a Twitter propaganda machine then let it loose on Coronavirus", *Propublica*, 26 March 2020.

Hypothesis

Our period of study covers tweets made between 3 October 2020 and 3 December. We focused our analysis on official CCP accounts in EU member states, as well as on prominent accounts that are not EU-based (e.g., MFA_China, SpokespersonCHN). Appendix 1 lists the 29 Chinese government accounts we considered. Our hypothesis was that Chinese government efforts to influence European public opinion on Twitter increased in the period immediately before and immediately after the US Presidential elections on 3 November 2020.

Methodology

To compile the dataset for our analysis, we submitted an application to Twitter to gain access to the Twitter API for Academic Research, to which we submitted a list of accounts that we wanted to analyse.[143] Once the application had been accepted, we started our trawling process on Twitter, using 3 October 2020 to 3 December 2020 as the time window. At first, we built a dataset (the *Hashtag dataset*) using hashtags related to the COVID-19 pandemic, EU-China relations and the 2020 US Presidential election. Our initial approach was to make the trawl and subsequent analysis process as simple as possible by focusing only on a few hashtags. We used the Google Translate API for English translations.[144] Table 1 shows the hashtags used and the number of tweets for the target accounts.

Hashtag	*Number of tweets*
2 WUHAN	86
China EU	5
COVID 19	3580
Liwenliang	0
US Election	22

Table 1: Number of tweets per hashtag in the Hashtag dataset

Table 1 shows that there were few tweets related to either the US Election or EU relations. The accounts rarely used hashtags to promote their tweets, or at least those considered in our analysis. We surmise that CCP representatives care less about using the Twitter trending algorithm but instead use the platform simply to project messages. As a result of the low returns on the hashtag search, we built a second dataset (the *Keyword dataset*)

[143] Academic research access, Twitter Developer Platform, https://developer.twitter.com/en/products/twitter-api/academic-research

[144] AutoML translation, Google Cloud, https://cloud.google.com/translate/automl/docs/

by using a keyword search to find relevant tweets from the target accounts. The keywords were selected based on our preliminary text analysis. Due to time constraints, we restricted our first search to keywords mainly related to the 2020 US election. We plan to extend the study to a wider and more targeted set of keywords in the next stage of the project. We also plan to enlarge the scope of our research to official PRC media accounts. Table 2 shows the number of tweets identified by each keyword in the Keyword dataset.

Keyword	*Number of tweets*
Biden	731
Donald	288
Donald Trump	210
Election Fraud	3
Fraud	31
Harris	54
Hegemon	36
Hegemony	26
Kamala	39
Kamala Harris	30
Liberal	21
Lies	279
Mike Pence	18
Misinformation	9
Pence	28
Presidential Elections 2020	1
Rigged	4
Stop the steal	1
Suspend	145
Trump	915
Unilateral	65
Unilateralism	39
United States	143
USA	346
Vote	389

Table 2: Number of tweets per keyword in the Keyword dataset

We found no tweets corresponding to the following keywords: EU-US, Transatlantic Relationship, Sleepy Joe, Settle for Biden, Democrats/Dems, Republicans/Reps/GOP, MAGA/Make America Great Again, Build Back Better, Keep America Great, Four More Years/4 More Years, Count the vote, Big steal, Rigged Election.

Findings

All the Twitter accounts that returned relevant tweets were examined. EU-based Chinese government-related accounts, such as embassies, consulates and the official named accounts of the ambassadors, were prioritised, followed by non-EU Chinese government accounts such as those of foreign affairs officials and spokespersons, and the Ambassador to the US. The number of relevant tweets made it possible to approach the retrieved data qualitatively, by reading and classifying each of them. In line with the research hypothesis, the goal was to examine whether efforts to influence European public opinion could be identified and whether there had been an increase in such efforts during the period immediately before or after the US Presidential elections of November 2020.

The analysed tweets contain both direct and indirect references to the US. The direct references are mostly related to the US position in the UN on human rights in China. For example, with reference to the UN General Assembly Third Committee's third meeting of the 75th session, which had taken place the previous day, tweets were published with slight variations across multiple official PRC accounts around 7 October.

"A small group of countries, led by the United States, Germany and the United Kingdom, abused the UN platform, politicized the issues of human rights and provoked confrontation"

Embassy of the People's Republic of China in Italy @Amb China (7 Oct. 2020)

Similarly, the Embassy of China in France has been very active and vocal about the UN events both in tweets, retweets and responses, posting that the US and their partners attempted *"to vilify the human rights situation in China"*, and retweeting the *People's Daily* French edition with an introduction:

"#United States threatens global political security by interfering in the internal affairs of other countries"

Embassy of China in France @AmbassadeChine (29 Oct. 2020)

Although not directly related to the election, this group of tweets, demonstrates the official PRC frame of presenting the US to audiences within the EU as an actor that does not respect national sovereignty.

A story on the economic benefits of the PRC market over the US can be interpreted as an attempt to tilt opinion in the EU member states and away from the US. For example, according to a tweet on 3 November:

'"The Chinese market is growing faster than our traditional export markets in Europe and the United States and takes a larger share of Danish total exports today than it did 10 or 20 years ago', says Danish economist"

Embassy of the People's Republic of China in the Kingdom of Denmark @ChinaInDenmark (3 Nov. 2020)

Another example of attempts at subtle influence is Chinese government efforts to highlight the importance of the EU's economic cooperation with China, especially during the COVID-19 pandemic:

"As of Nov. 5, China-Europe freight trains made more than 10,000 trips delivered 930,000 TEUs of goods this year. Serving as a key "cargo lifeline" connecting 21 countries & 92 cities in Europe, the China-Europe Railway Express has delivered over 60 tonnes of medical supplies."

ZHAO Lijian, MFA Spokesperson @zlj517 (18 Nov. 2020)

The second group of US-related posts contain indirect references. For example, CCP accounts avoid calling out the US directly and instead use proxy references, most notably hegemon, unilateralism, power politics and long-arm jurisdiction. A tweet of 12 November noted that:

"We need to adhere to peaceful coexistence. We need to uphold #multilateralism, oppose unilateralism, hegemony & power politics, and reject all forms of #terrorism and acts of extreme violence. We need to work together to safeguard equity, justice, peace and security in the world"

PRC Mission to the EU @ChinaEUMission (12 Nov. 2020)

In a response that ties the two topics of US interference and hegemony together, the Consulate General of China in Barcelona noted that:

"Xi expresses opposition to interference in internal affairs, unilateral sanctions and "long-arm jurisdiction"

Consulate General of China in Barcelona @ConsulChinaBcn (17 Nov. 2020)

The frame deployed in this context is that of calling on the EU to stand with China against the US.

Admittedly, none of these tweets by Chinese government representatives went viral, demonstrating the limited effect of China's frames on EU public opinion. What should be noted, however, is the presence and consistency of the anti-US frames tailored to the EU, which points to a PRC foreign policy rationale. In addition, even if the Chinese government's attempts at public diplomacy in the EU are not counted as successful by some measures, they could contribute to a broader undermining of trust and fuel doubts about European democracy and its effectiveness.

To conclude, we found that criticism of the US was indeed an identifiable topic in official PRC twitter communications, proving the first part of the hypothesis. We did not, however, find substantial proof to uphold the second part of the hypothesis: that such messaging peaked around the US Presidential elections on 3 November 2020.

Preliminary policy recommendations for the European Commission

- Strengthen EU influence campaigns to influence recent PRC emigres and virtual private network users in China by shaping information in a way that is not stylistically or linguistically foreign to this demographic; use simplified characters and mainland China vocabulary to emulate the approach PRC citizens are accustomed to.
- Work closely with traditional allies, such as the G7 and D10 countries, and non-traditional allies to better understand China's disinformation tactics.
- Strengthen the "Universal digital education and skills" aspect of the Digital Compass by funding campaigns across the EU member states to educate high school students (11–18yrs) specifically on how to engage more critically with social media in order to better identify attempts at disinformation and misinformation.
- Demand that Facebook, Twitter, YouTube and other large social media companies continue to

improve their identification, labelling and take down of disinformation on their platforms to prevent fake news from spreading.

Next Steps

This analysis is an iterative process that requires a blended approach between the technical expertise of big data analysis of social networks, and expertise on China and foreign policy in order to continuously refine the search results. A set of specific steps that could be taken forward by a multidisciplinary team is set out below.

- Break down the analysis to the EU member state level;
- Include state media accounts (CGTN, Global Times, Xinhua news) in the analysis;
- Examine a wider timeframe to establish peaks in messaging and determine whether these can be tied to specific events;
- Expand the list of keywords, adding "long-arm jurisdiction" and "power politics";
- Use automated mechanisms to discover relevant tweets that do not require (or limit) human intervention;
- Test more advanced tools for the retrieval of interesting tweets, in addition to keyword-based ones (e.g., using sentiment analysis and machine learning); and
- Establish whether there are links between global Chinese government accounts and Europe-based Chinese government representatives.

Appendix: List of Accounts

EU-based Chinese government-related accounts

Amb_ChenXu, AmbassadeChine, AmbCina, AmbLiuGuangYuan, China_Lyon, ChinaAmbNL, Chinaemb_Hellas, ChinaEmbEsp, ChinaEmbFinland, ChinaEmbireland, ChinaEmbNL. ChinaEmbSVK. ChinaEUMission, Chinain-Denmark, ChineseEmbinHU, Chnembaustria, ChnEmbGermany, Consulat_de, ConsulChinaBcn, GeneralkonsulDu, Li_xiaosi, LiuYanCHN, PRCAmbNL, RibiaoChen, YaoFei9

Non-EU based China government accounts

AmbCuiTiankai, MFA_China, SpokespersonCHN, Zlj51

Authors:
Una Aleksandra Bērziņa-Čerenkova is Head of the Riga Stradins University China Studies Centre and Head of the Asia Programme at the Latvian Institute of International Affairs (LIIA). Contact: una.berzina-cerenkova@rsu.lv
Elena Ferrari is a Professor of Computer Science and Director of the STRICT Social lab at the University of Insubria in Italy. Contact: elena.ferrari@uninsubria.it
Julia Voo is a non-resident Fellow of the Belfer Center for Science and International Affairs at Harvard Kennedy School. She is based in the United Kingdom. Contact: juliavoo@hks.harvard.edu


DPC

Power competition and China's technical standardisation

Maja Björk, Tim Rühlig

Abstract

In their chapter on technical standardisation, Tim Rühlig and Maja Björk argue that technical standards setting can translate into power in all four dimensions of the digital China challenge outlined above. China's influence on international standardisation is growing, creating challenges for EU interests in the form of politicisation, the risk of international bifurcation and shifts in power over technical standardisation. The paper makes three sets of policy recommendations on ways forward for an EU response to China's increased standardisation power. The strategic importance of technical standards, not least in the emerging competition over high technology, means that they will require strategic responses and even greater attention from the EU in the years to come.

The EU must ensure its technological sovereignty and be a global standard setter. Indeed, while technical by nature, standardisation is a highly strategic activity. In an increasingly competitive global environment, standardisation must support EU strategic autonomy and fundamental EU policy objectives. European Commission.

European Commission: "Roadmap. Standardisation strategy"

Three years ago, the members of a delegation of international technical standardisation experts, asked to provide advice on a new round of technical standardisation reform in the People's Republic of China (PRC), found itself in a meeting with China's Prime Minister, Li Keqiang, who spoke without notes for 20 minutes about the relevance of technical standards.[145] This was in stark contrast to the situation just a few years earlier, when such a visit would have been relatively low-status and involved meetings only with Chinese standards development organisations (SDOs) and officials. Technical standardisation, long absent from the power competition between states, has taken centre stage in the

[145] Information according to author interviews with European standardisation representatives.

strategic considerations of China, the United States (US) and the European Union (EU).

The centrality of technical standards is visible in core policy documents of both the PRC and the EU. In March 2021, China officially adopted its 14th Five-year Plan, which sets the framework for the next five-year planning cycle.[146] While general in character, a mention of technical standards in almost one-third of its chapters is a clear indication that China intends to prioritise technical standardisation in the years to come.[147] In October 2021, China published a new national technical standardisation strategy that underlines the strategic importance the PRC attributes to technical standards. The strategy was published not only by the State Council, but also by the Central Committee of the Chinese Communist Party (CCP). It could hardly have been made any clearer that this document had the highest priority, and the blessing of China's senior leadership. The strategy also demonstrates a shift in China's standardisation ambitions. Until then, it was the domestic angle of standard setting that was prioritised, but China is now giving equal weight to its international ambitions. Furthermore, by stating that standard setting should help the PRC to increase supply chain security, China has put standardisation in the context of the geopolitical rivalry over high technology.[148]

The EU is also developing a technical standardisation strategy.[149] It is seeking to improve the EU standardisation system and to develop a more strategic approach to international standardisation, which includes safeguarding EU values and strengthening European influence. The EU's 2030 Digital Compass reflects the relevance of technical standards and highlights an intention to cooperate with like-minded partners in this field.[150] Most prominently, the EU-US Trade and Technology Council (TTC), launched early in 2021 to facilitate EU-US coordination on global trade, economic and technology issues, is set to include a technical

[146] See introductory chapter of this report.

[147] Xinhua, "（两会受权发布）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*, accessed 3 April 2021, at http://www.xinhuanet.com/2021-03/13/c_1127205564.htm.

[148] People's Republic of China, "中共中央 国务院印发《国家标准化发展纲要》", *Standards Administration of China*, accessed 20 October 2021, at http://www.gov.cn/zhengce/2021-10/10/content_5641727.htm.

[149] European Commission, "Shaping Europe's Digital Future", *European Commission*, accessed 29 August 2021, at https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf; European Commission, *Updating the 2020 New Industrial Strategy: Building a Stronger Single Market of Europe's Recovery. Communication form the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2021) 350final*, Brussels, *European Commission*, 2021.

[150] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 2030 Digital Compass: the European Way for the Digital Decade. COM(2021) 118 final", *European Commission*, accessed 2 April 2021, at https://ec.europa.eu/info/sites/info/files/communication-digital-compass-2030_en.pdf.

standardisation cooperation working group.[151] This increased prominence of technical standards in Chinese and EU policy documents raises three questions, which are addressed in this chapter:

1. How does influence over technical standardisation translate into power?
2. In what way does China's standardisation power pose a challenge for the EU?
3. How should the EU respond to China's growing standardisation power?

The chapter ends by highlighting three important areas in need of future research, which would enable the EU to better understand and be better prepared to respond to China's standardisation power.

How does influence over technical standardisation translate into power?

Technical standards are omnipresent and, due to an increasingly digitalised economy, more crucial than ever for EU competitiveness. Increasing connectivity requires greater interoperability and complementarity of technologies and products, which is one of the primary functions of technical standards. Understanding technical standards in a geopolitical context, however, is less intuitive.

Technical standards are *voluntary* product specifications, achieved either as a result of market dominance (de facto standards) or development by SDOs, which are made up overwhelmingly of representatives of private sector industries. While public sector actors play a minor role, technical standardisation is largely an example of *private sector self-regulation*. Technical standards apply a very different logic than, for example, export controls or punitive tariffs, which aim to exclude competitors or prevent market access, and are being used by the US and China in their emerging technological competition. The political impact is also not obvious due to the *technical nature* of these standards. For example, USB is a standard for cables, connectors and protocols that enables charging and the exchange of data on a wide range of devices. Why does it politically matter who developed the technology for such standards?

We argue that the political relevance of technical standards plays out in the same four dimensions identified by the Digital Power China research consortium as the four features of the digital China challenge (see introductory chapter).[152]

Economic dimension: Technical standards have significant distributary effects, resulting from the fact that patented

[151] European Commission, "EU-US launch Trade and Technology Council to lead values-based global digital transformation", *European Commission*, accessed 29 August 2021, at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990.

[152] See introductory workshop paper by Rogier/Fischione/Rühlig.

technologies constitute a large proportion of technical standards. In the field of Information and Communication Technology (ICT) standards, an estimated 55% of the technology used is patented.[153] When patent holders declare patents to be standard-essential (standard-essential patents, SEPs), they commit to making them available through licensing on fair, reasonable and non-discriminatory (FRAND) terms. FRAND terms may sound utilitarian, but can generate considerable royalties. The US technology company Qualcomm, for example, earned around 20% of its revenue from patent licensing in 2017.[154] Furthermore, companies that succeed in including their technology in technical standards gain from avoiding the adaptation costs that arise when a company must redesign its products to comply with the new standard. In the words of Werner von Siemens, back in the late 19th century, "he who owns the standards, owns the market".[155]

Legal dimension: While legally voluntary, standards can have enormous legal force. Several agreements within the framework of the World Trade Organisation (WTO)[156] treat international standards as benchmarks for the facilitation of international trade. If domestic technical standards deviate from international ones, in principle, unless a reasonable explanation can be provided for deviation, the judiciary at the WTO could declare a state noncompliant with the law on international trade. Roughly 80% of international trade is affected by technical standards and technical regulations.[157] Domestic technical standards can also have extraterritorial effects. States can reference technical standards in legal documents as suggested methods for meeting legal requirements. When applied, the product can assume conformity with the regulations. Implementing the standard is therefore often the easiest and cheapest option. Multinational companies often choose to comply with the strictest technical standards since this generates conformity with regulations and therefore access to all relevant markets. Thus, when standards are referenced in the regulations for major markets, such as the European Single Market, the US or the PRC, they have effects beyond these territories.

Security dimension: Global technical standards facilitate interoperability across borders. If contradictory technical standards exist in different geographical locations, however, they generate distinct technological spaces. One result

[153] Tim Pohlmann, *Back To Basics Summer Webinar Part 2: SSOs, Patent Pools and Licensing*, Berlin, IPlytics, 2020.
[154] Dan Strumpf, "Where China Dominates in 5G Technology", *Wall Street Journal*, accessed 13 April 2019, at https://outline.com/dVsKLJ.
[155] Werner von Siemens quoted in: Hermann J. Koch, *Practical Guide to International Stanardization for Electrical Engineers. Impact on Smart Grid and e-Mobility Markets*, New Jersey, Wiley, 2017. p. xix.
[156] Such as the Agreement on Technical Barriers to Trade (TBT), the Agreement on Government Procurement (GPA), the review of the Agreement on Sanitary and Phytosanitary Measures (SPS), and the General Agreement on Trade in Services (GATS).
[157] OECD, *Regulatory Reform and International Standardisation. Working Party of the Trade Committee. TD/TC/WP(98)/FINAL*, Paris, OECD, 1999.

can be lock-in effects, which occur when country A adopts the standards of an industry in country B, and only suppliers in country B produce compatible technology. Studies have demonstrated that high switching costs lead to the preservation of dominant technical standards.[158] Lock-in effects in critical sectors, such as infrastructure, can have serious political implications. If all the suppliers that use the particular technical standards are based in country B, it could use this as leverage to pressure country A for political concessions in return for continued supply, maintenance and build out of the infrastructure in question. Even in the absence of explicit requests, country A would think twice before adopting a confrontational stance on issues of core interest to country B. Technical standards can also have implications for cybersecurity, based on the assumption that those that develop a standard could have a deeper knowledge of its technology, including vulnerabilities. The Snowden disclosures, for example, provided evidence of how the US National Security Agency (NSA) has worked to build backdoors into encryption standards.[159] If adopted as an international standard, the technology spreads globally.[160] Other observers argue that the transparent processes of standardisation make it almost impossible to hide security-relevant flaws from the eyes of the engineers of potential adversaries. From this perspective, a high degree of standardisation increases cybersecurity by means of transparency.[161]

Ideational dimension: How technology is designed is highly political as it is inscribed with ethical values as part of the process. Technical standards determine what is perceived as "normal" technology and contribute to the constitution of our social lives. For instance, Wi-Fi is seldom questioned as the dominant wireless area network (WLAN) standard but, just a few years after Wi-Fi was established as the international standard, China proposed WAPI technology as a new standard. WAPI promised better performance but provided weaker privacy. Whether intended or not, by rejecting WAPI, international SDOs prioritised privacy over performance, shaping what consumers expect from WLAN technology. Whoever sets the technical standards on algorithmic bias, data privacy and similar issues will shape the ethical, political and security functions and expectations of key enabling technologies.

[158] W. Brian Arthur, "Competing Technologies, Increasing Returns, and Lock-in By Historical Events", *The Economic Journal* 99 (394), 1989, pp. 116-131. Joseph Farrell and Garth Saloner, "Standardization, Compatibility, and Innovation", *Rand Journal of Economics* 16(1), 1985, pp. 70-83.

[159] Michael Rogers and Grace Eden, "The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures", *International Journal of Communication* 11 (1), 2017, pp. 802-823.

[160] Roma Eisenstark, "Why China and the US Are Fighting over 5G", *TechNode*, accessed 11 April 2019, at https://technode.com/2018/03/30/5g/; Milo Medin and Gilman Louie, *The 5G Ecosystem. Risks & Opportunities for DoD*, Washington DC, Defense Innovation Board, 2019.

[161] Author interviews with European engineers involved in the development of 5G. February-November 2019, several cities.

In what way does China's standardisation power pose a challenge to the EU?

China's influence over international technical standardisation is growing – both through its presence in international SDOs and de facto through standardisation linked to growing market share and as part of the Belt and Road Initiative (BRI).[162] In addition to credible reports by the international standardisation community, a broad range of statistics illustrates China's growing role (see Figures 1–6).

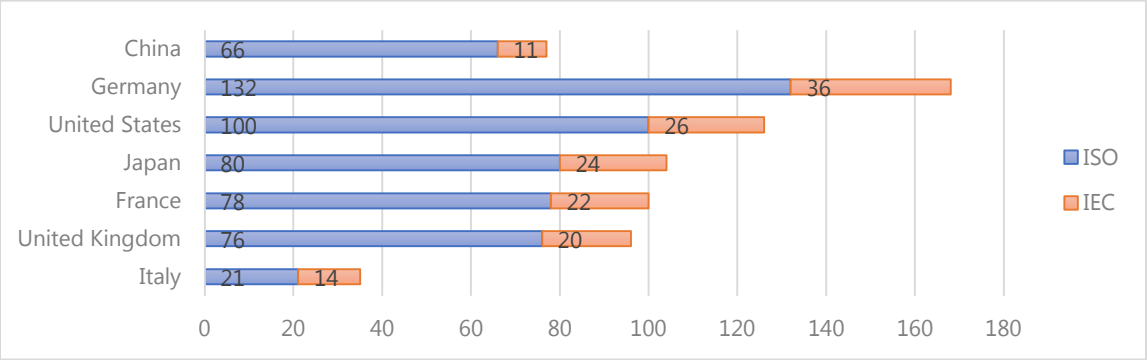

Figure 1: Secretariat positions in the International Organisation for standardisation (ISO) and the International Electrotechnical Commission (IEC) as of April 2021, selected countries. Source: ISO, IEC

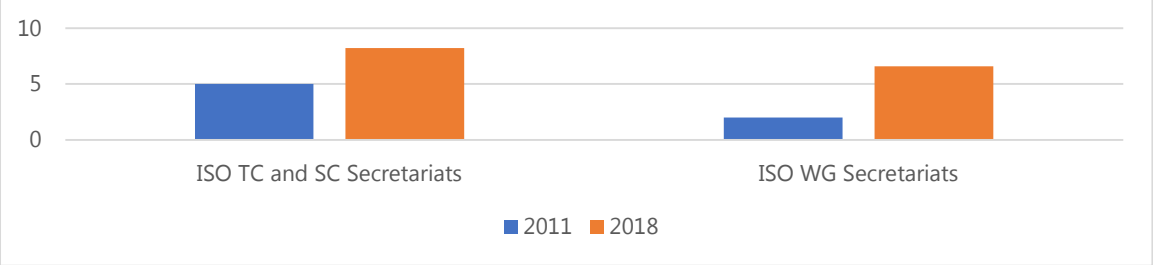

Figure 2: Share of Chinese ISO secretariat positions (%). Source: DIN.

[162] Tim Rühlig, "*China's Technical Standardisation Power. Implications for the European Union. Non-public report*", Brussels, European Commission, 2020.

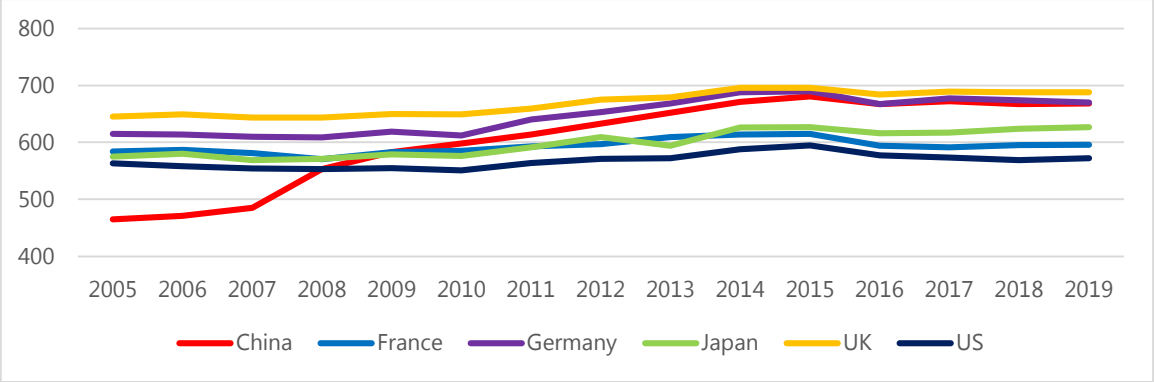

Figure 3: Active memberships of ISO Technical Committees and subcommittees, selected countries. Source: Data obtained from AFNOR.

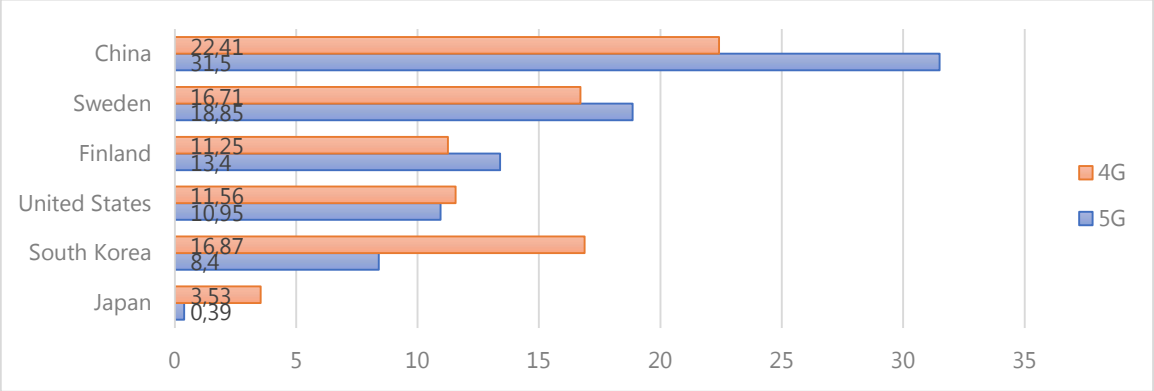

Figure 4: Share of standard contributions (%). Comparison of 4G and 5G technology standard as of January 2021, selected countries. Source: IPlytics

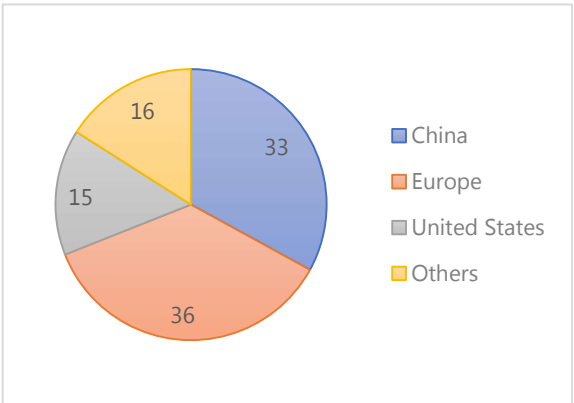

Figure 5: Share of standard contributions (%) to the Third Generation Partnership Project (3GPP) – a group of international SDOs in the telecommunications field – in 2018, selected countries. Source: Own calculation based on privately obtained data.

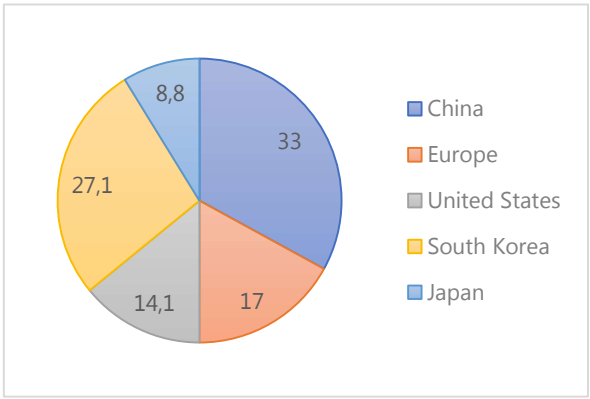

Figure 6: Share of SEP declarations (%) as of January 2020, selected countries. Source: IPLytics

The EU faces three overlapping sets of challenges emerging from China's growing standardisation power: the politicisation of standard setting, a bifurcation of international technical standardisation and power shifts in standardisation.

Politicisation: The Chinese party-state's strategic approach to international standardisation – coupled with the emerging power competition over high technology – is leading to a politicisation of technical standards. China's growing footprint could also lead other, primarily developing countries, to consider adopting a state-steered approach to standard setting.[163] This stands in sharp contrast to, and risks undermining, the EU's successful private sector-driven Public-Private Partnership model of technical standardisation.[164] Politicisation alters the character of standardisation by incorporating a focus on which actors, from which political contexts, are involved in international technical standard setting. In strategic sectors, Chinese firms profit from party-state support in the form of soft loans for investments in research and development, preferential treatment in public procurement (in one of the world's largest markets), and even direct financial subsidies for standard development. While technical standards have long included an ideational dimension, the recent politicisation could substantially alter the standardisation process. Actors might start paying increased attention to the political, ethical and societal underpinnings of technological solutions, thereby turning standardisation into an arena for political competition.

Bifurcation: As a result of politicisation, international standardisation risks being divided into two camps. China could aim to develop a rival system for international standard setting, and the BRI could serve as its stepping stone to outcompete established standardisation powers such as the EU member states and the US. The PRC is a latecomer to the existing institutional system. Established standardisation powers are striving to preserve the system and integrate China into it without losing influence, but this is trying to square the circle. China, as a novice in the game, is aiming to learn how to play its cards right in order to stretch the rules, or even change them. For example, China Standards 2035, a research initiative funded by the Chinese party-state, has suggested the establishment of a BRI Regional Standards Forum. This forum could help China rally support from developing countries for its interests in ISO and IEC, or even issue new types of international standards, possibly indicating the creation of a new international institution that would undermine existing international standards and standardisation. Although China's standardisation strategy does not mention such a forum, this might only indicate that the PRC leadership has

[163] Tim Rühlig and Tobias Ten Brink, "The Externalization of China's Technical Standardization Approach", *Development & Change* forthcoming, pp.

[164] Tim Rühlig, *Technical Standardisation, China and the Future International Order: A European Perspective*, Brussels, EU Office of the Heinrich Böll Foundation, 2020.

not yet come to a consensus on whether to establish such an institution. A multitude of SDOs are already competing for international influence, but ISO and IEC are the key platforms that account for around 85% of all international product standards.[165] Any bifurcation would also facilitate lock-in effects. A further concern is that technical standardisation could become an arena for a new Cold War with two distinct blocs competing over the values inscribed in technology. China's expressed intention to invest in facial recognition standards,[166] for example, and its proposal for a reformed standard Internet protocol, referred to as New IP,[167] have alarmed experts in Europe and the US. The fear is that political and ethical preferences shaped by the PRC's political and societal framework will spread through the internationalisation of Chinese standards.

Power shifts: Established international standardisation powers, primarily the EU, fear that their impact on international standard setting is diminishing. In addition, the force of standards themselves could also dwindle. Economically, a redistribution of resources is at the centre of power shift concerns. Actors that are used to gaining a large share of the royalties from SEPs could face higher adaptation costs and licensing fees for the use of technology by Chinese competitors, thereby also limiting their ability to invest in new research and innovation. A likely reaction is that groups of like-minded actors will engage in policy coordination in order to speak with one voice. This can already be seen in China. While the unity of the party-state and its political economy is often overestimated,[168] by international comparison – particularly in a field of national priority such as 5G – there is a fairly high degree of national coordination and cohesion. A prime example of such coordination is the IMT 2020 (5G) Promotion Group, which brings together Chinese public agencies, research institutes and Chinese tech companies.

How should the EU respond to China's growing standardisation power?

The EU's response to China's increased influence in technical standardisation should address these three challenges. This section provides three corresponding sets of policy recommendations. It is worth noting that while our

[165] Tim Büthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy*, Princeton, Princeton University Press, 2011.

[166] Yujie Xue, "27 Companies Drafting China's First National Facial Recognition Standard", *Sixth Tone*, accessed 4 April 2020, at http://www.sixthtone.com/news/1004893/27-companies-drafting-chinas-first-national-facial-recognition-standard.

[167] Madhumita Murgia and Anna Gross, "China and Huawei Propose Reinvention of the Internet", *Financial Times*, accessed 30 April 2020, at https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2.

[168] Ashley Feng, "We Can't Tell if Chinese Firms Work for the Party", *Foreign Policy*, accessed 15 February 2019, at https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/.

recommendations primarily address EU policymakers and the European Commission, there are other relevant actors that would play a role in an effective European response to China's standardisation power. At the industry level, for example, efforts could be made to increase awareness and discussion of the role and increasing strategic importance of standardisation among European CEOs and company leaderships.

Respond to the politicisation: The EU should certainly maintain its private sector-driven Public-Private Partnership, which has made it a global technical standardisation power. However, at a time when technical standards are becoming the subject of political competition, the EU needs to systematically coordinate its strategic priorities and advocate a non-political approach.

1. *Facilitate a three-layered strategic "foresight dialogue" on standardisation within the EU:* At least once a year, all EU member states and the European Commission should meet for a dialogue on technical standardisation, with the specific purpose of identifying and coordinating strategic goals and concerns in the field of standardisation from the perspective of public authorities. This dialogue should start by seeking consensus on strategic sectors such as 5G, AI, the IoT, quantum technologies, semiconductors and robotics [layer 1]. In direct conjunction, the same public representatives should engage in a joint dialogue with European standardisation organisations (ESOs) and national standardisation bodies (NSBs) to communicate their strategic priorities (top-down) and better understand the challenges facing the SDOs (bottom-up). This dialogue, which would resemble some elements of previous EU initiatives,[169] should help to align strategic and industry interests [layer 2]. The European Commission should further sponsor coordinated information exchange forums for the ESOs, NSBs and European industry, similar to China's IMT 2020 (5G) Promotion Group, to prepare international standardisation on specific standards of strategic importance [layer 3].
2. *Focus standardisation cooperation in the EU-US Trade and Technology Council on coordination:* Two core challenges for the technical standardisation working group of the TTC are that technical standardisation on both sides of the Atlantic is private sector-driven, with limited public influence, and has very different standardisation systems. Hence, the TTC working group should primarily serve a coordination

[169] Such as the Multi-Stakeholder Platform on ICT standardisation (MSP) or the Joint Initiative on Standardisation (JIS).

function on new technologies and communicate strategic goals similar to the "layer 1" dialogue above.

3. *Invest in standardisation knowledge:* In 2020, the United States invested $US 1 million in a National Institute of Standards and Technology (NIST)[170] study of China's technical standardisation efforts in new technologies. Similarly, Australia has dedicated $US 5.9 million to understand how to boost Australia's influence over international standardisation. The EU should follow such examples and investigate in more detail the political implications of standardisation in concrete sectors and contexts, such as China's BRI.
4. *Incentivise international standards in connectivity initiatives:* States along the BRI are becoming increasingly aware that incorporating Chinese technical standards comes with technological dependencies. The EU should tap into the growing unease, and incorporate and incentivise the use of international standards in all the financing vehicles it is involved in, primarily its new "Global Gateway" initiative. Success will depend, not least, on the EU's financial contributions.

Preventing bifurcation: To avoid a decoupling of standards, the EU should continue to cooperate with China wherever possible, but be clear about international rules and demand reciprocity.

5. *Target subnational actors in China to advocate for the European standardisation approach:* The CEN-led Seconded Standardisation Expert in China (SESEC) explains and advocates for the European approach to technical standardisation. This project should receive additional funds to extend it to subnational and industry players and create momentum beyond the central party-state authorities to adopt more aspects of the European approach.
6. *Continue offering support for a "Beijing" and a "Shanghai Agreement":* China has voiced careful interest in exploring "Beijing" and "Shanghai Agreements" with ISO and the IEC, resembling the European "Vienna" and "Frankfurt Agreements" set up to avoid duplication of and strengthen international standards. China's new standardisation strategy also expresses an intention to increase the adoption and conversion of international standards. The EU should continue to use its experience and knowledge to facilitate such Chinese efforts.
7. *Make automatic sanctions part of the EU's WTO reform proposal:* Despite progress, China still falls

[170] NIST is a science laboratory and non-regulatory agency of the US Department of Commerce.

short of its reporting duties on technical standards to the WTO Technical Barriers to Trade Committee. The EU should not only continue to raise this subject in its dialogues with China, but also make automatic sanctions for violation of reporting duties part of its WTO reform proposal.

8. *Address challenges to certification:* The EU should continue to demand recognition of international certification in China, such as IEC testing for GB standard conformity assessment.[171] Moreover, the EU foreign investment screening mechanism should explicitly include Notified Bodies in order to avoid Chinese takeovers in critical sectors with a high market concentration of Notified Bodies, particularly in the smaller EU member states.[172]

Preserving the EU's technical standardisation influence: The EU should consider a broad range of measures to strengthen its standardisation power. Some would directly tackle the shortcomings of standardisation while others, such as strengthening innovation through competition or providing reliable digital infrastructure as a precondition for digital innovation, would indirectly promote the EU's influence on standardisation. Our recommendations below address standards more directly.

9. *Incentivise the development of technical standard proposals within Horizon Europe:* The EU should make the development and submission of technical standard proposals alongside publications and patents deliverables of Horizon Europe funding. Pre-normative research could also take centre stage in Horizon Europe calls.
10. *Support academic standardisation education:* In China, thousands of engineering students graduate every year from programmes that either exclusively train them in technical standardisation or include modules on standardisation. In Europe, engineers normally learn about standardisation only once they are working as industry representatives in technical standard setting committees. The EU should, wherever possible, provide funds for academic standardisation education that is practice-oriented and not too abstract and theoretical.
11. *Support SMEs and civil society actors:* Technical standards are mainly developed by big

[171] GB standards are Chinese national mandatory standards relevant for market access.

[172] Zhong Nan, "Certification firm gets nod as central SOE", *China Daily*, accessed 2 September 2021, at https://govt.chinadaily.com.cn/s/202006/12/WS5ee2ebcc498ed1e2f340711d/certification-firm-gets-nod-as-central-soe.html; Parliamentary questions, "Subject: Risks arising from foreign takeovers of Notified Bodies", *European Parliament*, accessed 2 September 2021, at https://www.europarl.europa.eu/doceo/document/E-9-2021-001186_EN.html.

companies. Our own statistical analysis suggests, however, that when small and medium-sized enterprises (SMEs) engage in standardisation, they have a higher success rate. The EU should provide additional earmarked funding via Small Business Standards (SBS) to support SME participation in standardisation, particularly at the international level. Relatively small amounts can create incentives and help strengthen European influence. Similarly, financial support for societal stakeholders would be helpful, not least because these actors tend to be freer to address the ideational dimension of standard setting. They have no business interests to consider in China or in relation to other companies, or political pressures that might prevent them from speaking up against Chinese proposals. The EU member states could also play an important role by more clearly promoting and acknowledging the importance of social interests in standardisation.

12. *Support early commercialisation with funds and regulation:* The EU is still relatively strong in research and innovation but faces challenges with early commercialisation. For critical new technologies, the EU should consider setting up a special support framework, to which entrepreneurs can submit their innovations for scientific review and apply for temporary exemptions from certain regulations that impede timely commercialisation, while also – if required – applying for funds to bridge the "valley of death" between innovation and commercialisation. Such support could help facilitate new technological innovation and faster market deployment, both of which are favourable early steps for standardisation. The review could assess innovativeness, the prospects for market success, the potential to serve EU strategic interests and the public good, and the risks if regulation is temporarily suspended.

Finally, and more generally, the EU should make standards a default part of the EU's trade policy and consider standardisation as one of several important issues when deciding on competition law reform.

Future research

In recent years, a number of studies have contributed to a better understanding of China's general approach to technical standard setting.[173] However, many aspects remain to be researched. We highlight three areas that require further investigation:

- *Continuous tracking of Chinese standardisation activities:* While general analyses of China's standard setting approach can provide an important overview, these are not enough for the purposes of predicting and preparing for developments in concrete standard contributions. In the recent past, Europe has too often been surprised by Chinese standard contributions, such as in the field of lithium batteries or a new Internet protocol. A continuous tracking of Chinese standardisation activities is necessary in order to avoid similar situations in the future. Such tracking should consist of three components: (a) close coordination and information sharing with European industry; (b) scientific analysis by technical experts; and (c) contextualisation of information and analyses in the broader context of Chinese digital, industrial and foreign policymaking. One of the intentions outlined in China's new standardisation strategy is to continue to promote standards drafting in key technologies. This only emphasises the need for better tracking of such activities.
- *Standardisation in specific emerging technology fields:* Another important element that general analyses are not able to capture is a deeper understanding of standardisation activities in specific technological fields. Standard setting differs in its practices, institutions and developments between technological sectors, which means that knowledge about one standardisation sector far from ensures knowledge about another. More studies are needed of Chinese standard setting activities in specific sectors, such as AI, in order to understand China's strategies, practices and positions within different strategic standardisation ecosystems.
- *Standards in BRI projects:* Technical standards play a significant role in BRI projects and the recently published Chinese standardisation strategy provides an indication that this will continue to be the case in the future.

[173] Tim Rühlig, *The Shape of Things to Come: The Race to Control Standardisation*, Beijing, European Union Chamber of Commerce in China, 2021; Tim Rühlig, *Technical Standardisation, China and the Future International Order: A European Perspective*, Brussels, EU Office of the Heinrich Böll Foundation, 2020; John Seaman, *China and the New Geopolitics of Technical Standardization*, Notes de l'Ifri, Paris, Ifri, 2020.

Nonetheless, we still have very little data on standards in concrete projects, and such research is labour, time and resource intensive. Even so, it deserves serious effort, not least in the light of the EU's new "Global Gateway" initiative, in order to understand how precisely standards play out in competing BRI projects and in the context of China's international standard setting influence and ambition.

Standardisation is of enormous strategic importance and requires even more attention than it has received in recent years.

Authors:
Maja Björk is a MSc student at the University of Uppsala in Sweden. Contact: Maja.Bjork.1257@student.uu.se
Tim Rühlig is a Research Fellow at the German Council on Foreign Relation and an Associate Research Fellow of the Swedish Institution of International Affairs' Europe program. He is based in Germany. Contact: ruehlig@dgap.org


DPC

Projecting digital power internationally: Europe's digital China challenge

Brigitte Dekker, Maaike Okano-Heijmans

Abstract

This chapter highlights the consequences of China's digital power projection for the EU, especially in China's backyard – a region the EU now calls the Indo-Pacific – and in the EU's own neighbourhood of Africa, Central Asia and the Western Balkans. China's moves will require the EU and its member states to adopt an integrated approach that connects the dots between the digital agenda, the connectivity agenda – now known as the Global Gateway – and its policies on priority regions. The chapter's four policy recommendations encompass all the dimensions of digital connectivity: (a) invest in market and standard-setting power to complement the EU's regulatory power; (b) prioritise the Indo-Pacific region and Africa; (c) develop issue-based co-operation networks and digital governance that put people first; and (d) invest in digital development assistance and capacity building.

It is in the EU's best interests to act now on the opportunities and disruptions that are accompanying the global digital transition and transformation. As European Commission President Ursula von der Leyen put it in September 2020: "Europe must now lead the way on digital – or it will have to follow the way of others, who are setting these standards for us".[174] She added: "We must make this 'Europe's Digital Decade'". In March 2021, the European Commission presented a vision, targets and avenues for a successful digital transformation of Europe in its *2030 Digital Compass: the European way for the Digital Decade*, in which the four cardinal points of the compass are skills, government, infrastructure and business. The Global Gateway strategy of December 2021 added

[174] European Commission, State of the Union address by President von der Leyen at the European Parliament Plenary, accessed 5 September 2021, at https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655.

an ambition to support an open and secure internet beyond EU borders.[175]

The risks of failing to act on the Digital Decade have been laid bare by the COVID-19 pandemic. As governments resort to – sometimes intrusive – digital tools to monitor and combat the novel coronavirus, digital freedom of speech, transparency and inclusiveness are at stake. At the same time, innovative approaches to research and development, and the commercialisation of innovation will be needed to uphold economic competitiveness in the digital age. The pandemic has reaffirmed the need for improved resilience at home, as well as cooperation among like-minded partners that wish to protect and promote an open and inclusive cyber domain.

China's moves in the digital domain warrant closer scrutiny, as they fuel concerns about the sustainability of European ideas on digital sovereignty, a data-driven society, individual privacy and free flows of data. China's digital power projection globally also warrants attention, but the EU's particular focus should be on two regions where China's presence has been most substantial and the stakes for the EU are the most significant: the Indo-Pacific and the Europe's neighbourhood.

As we witness a power shift to the Indo-Pacific, the EU and its member states are pivoting towards this region, as demonstrated by the EU Indo-Pacific strategy published in September 2021. Geographically, the region is China's backyard, and therefore an obvious first choice for overseas expansion by Chinese companies. The Indo-Pacific is the fastest-growing digital economy and will be host to 90 per cent of the new middle class by 2030. The societal impact of disruptive technologies will therefore be particularly great in the region. In addition, the EU's own neighbourhood is important because of its geographical proximity and China's growing activism in Africa, Central Asia and the Western Balkans. When African governments turn to China for affordable digital solutions, interconnectivity and interoperability – and, hence, the adoption of European standards – are at stake. Understanding of and action in these regions is therefore of particular importance for the EU and its member states.

This chapter aims to increase awareness of China's digital power projection, especially in its own backyard and Europe's neighbourhood, and to enhance the debate in Europe about the trade-offs between individual, state and business interests in all subsets of what the EU has labelled "digital connectivity".[176] This

[175] European Commission, "The Global Gateway", Press release, accessed 12 March 2021, at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6433.

[176] In so doing, the paper builds on earlier (co-authored) publications by the author, notably the Clingendael Reports: Dekker, B. and Okano-Heijmans, M., "Unpacking China's Digital Silk Road", *Clingendael Institute*, accessed 1 September 2021, at https://www.clingendael.org/sites/default/files/2020-07/Report_Digital_Silk_Road_July_2020.pdf; Dekker, B. and Okano-Heijmans, M., "Europe's Digital Decade? Navigating the global battle for digital supremacy", *Clingendael Institute*, accessed 1

broad field covers a wide range of topics related to digital regulation, the e-economy and telecommunications infrastructure.

The four policy recommendations highlighted in this paper encompass all the dimensions of digital connectivity: (a) invest in market and standard-setting power to complement the EU's regulatory power; (b) prioritise the Indo-Pacific region and Africa; (c) develop issue-based cooperation networks and digital governance that put people first; and (d) invest in digital development assistance and capacity building.

Increased awareness and more debate among European stakeholders are needed to achieve a more sustainable EU approach that will outlast the current decade. After all, economic competitiveness is essential to securing Europe and to furthering its principled approach to digital connectivity in the long term. This paper is a first attempt to deliver on these objectives, and presents the contours of a future research agenda for interdisciplinary research on the topic by Sinologists, technical experts and policy-oriented international relations experts.

Digital China challenge

The rising power of China poses several challenges for the EU. *Economically*, an unlevel playing field favours Chinese tech firms that benefit from substantial state support and lower data protection and environmental standards. This advantage endangers the EU's digital industrial competitiveness. *Politically*, the Chinese government – in pushing the objectives of the Chinese Communist Party (CCP) – can leverage political concessions from technologically (over-)dependent third countries, including some EU member states. China's officials and private sector representatives are also actively engaging with global cyber-governance bodies to rewrite institutional processes and increase their power. In the *security* field, the inclusion of Chinese digital equipment could come with cyber-insecurities that enable espionage and sabotage by a state with which the EU has no security alliance. *Ideationally*, the technological footprint and penetration of Chinese companies in international markets call into question whether the governance principles of these digital technologies reflect liberal and democratic values – for example of an open, transparent and inclusive digital domain

September 2021, at https://www.clingendael.org/sites/default/files/2020-10/Report_Europes_digital_decade_October_2020.pdf; Okano-Heijmans, M., Nachiappan, K. and Dekker, B., "Fostering digital connectivity in and with the Indo-Pacific: Opportunities for the EU", *European External Action Service*, accessed 2 September 2021, at https://www.clingendael.org/sites/default/files/2021-04/Report_Digital_Connectivity_IndoPacific_April_2021.pdf; and Okano-Heijmans, M. and Vosse, W., "Digital connectivity going global: the case for digital ODA", *Clingendael Institute*, accessed 2 September 2021, at https://www.clingendael.org/sites/default/files/2020-05/PB_The_case_for_digital_ODA_May_2020.pdf.

that maintains high standards of privacy for its users. The concerns of the EU and its member states about how Chinese companies operate overseas are directly linked to the Chinese government and the stronghold of the CCP. It is evident that China is moving to position itself as the pre-eminent global digital power. The Digital Silk Road (DSR) is a key component of this ambition. It essentially combines a domestic push to export Chinese technologies, developed with assertive industrial policies and in a favourable regulatory context,[177] with a broader agenda to augment interoperability and compatibility between Chinese and overseas technological networks, on Chinese terms.

The DSR adds an extra dimension to China's Belt and Road Initiative (BRI), beyond its traditional infrastructure focus, and puts China's aspirations to lead the Fourth Industrial Revolution on full display. Building on the successes of its domestic industrial strategy, China has made significant steps to further the implementation and use of Chinese technologies in BRI participating countries, especially in China's backyard of South and Southeast Asia, and in Africa. This has set the stage for China to push its own standards as the Fourth Industrial Revolution unfolds: standards that display characteristics of what some experts refer to as "digital authoritarianism".[178] Thus, the DSR is an economic, political and ideational challenge to the EU.

The 14th Five-year Plan, adopted on 11 March 2021, has been designed with a keen eye on enhancing China's digital influence.[179] The plan has a clear focus on China's domestic economy, which the document refers to as the "internal cycle". While "decoupling" is not part of the Plan, the primary goal is to boost the resilience of the Chinese economy so that it can insulate itself from international instability and rivalries. In support of this goal, the current Five-year Plan is intended to reduce China's reliance on foreign technology, modernise its manufacturing and stimulate technological innovation. A new emphasis is also placed on digitalisation, as a large section of the plan is dedicated to finding new applications for digital technology in the economy and in government functions. Although many of the key projects outlined in the plan are still largely traditional infrastructure projects, there is a new emphasis on research, and Artificial Intelligence, quantum science and cloud computing are all mentioned. Thus, the 14th Five-year plan underlines China's ambition to become a global digital

[177] The key domestic initiatives and regulations are Made in China 2025, China Standards 2035, Internet Plus, the Cybersecurity Law, the Data Security Law and the 14th Five-year Plan (see below).
[178] Dekker, B. and Okano-Heijmans, M., "Unpacking China's Digital Silk Road", *Clingendael Institute*, accessed 1 September 2021, at https://www.clingendael.org/sites/default/files/2020-07/Report_Digital_Silk_Road_July_2020.pdf.
[179] Grünberg, N. and Brussee, V. "China's 14th Five-Year Plan: Strengthening the domestic base to become a superpower", *MERICS,* accessed 3 September 2021, at https://merics.org/en/short-analysis/chinas-14th-five-year-plan-strengthening-domestic-base-become-superpower

powerhouse and increase international dependence on Chinese technology.

The recent tensions over 5G hardware and the Chinese digital giant Huawei have been at the centre of the discussion and may be a harbinger of digital and technological showdowns to come. This competition is the result of China having gained an edge in 5G technology, which the West initially had difficulties in matching. Former US President Donald J. Trump's forceful moves to block Chinese 5G infrastructure,[180] and weaken Huawei internationally, showed China that it must prioritise innovation and the domestic market – two points that are highlighted in the current Five-year Plan. Beyond this, China is pushing its agenda in the field of smart cities, space and undersea cables by introducing its own alternative to GPS, helping countries to launch Chinese satellites, and supporting private sector investment in seabed cable projects and landing stations. These technologies, and of course 5G hardware, should all be considered critical infrastructure and shielded from potential Chinese influence or infiltration, as the risk of cyber-espionage should not be overlooked. These economic and political challenges must be countered with strong support for European innovation and homegrown alternatives to Chinese technology.

The Chinese government has also raised its game on the *ideational* challenge with the introduction of its "Outline for National Standardisation Development",[181] to which China Standards 2035 contributed. The document represents a blueprint for the drafting of global standards for the next generation of technology that logically builds on China's Made In China 2025.[182] Beijing is therefore well on the way to establishing itself as a leader in the digital age, with an approach that is characterised by a more state-centred and less open and transparent vision, in which individual rights are secondary to collective and state interests.

To this end, the Chinese government and Chinese companies are strengthening their presence in international organisations. This is being complemented by activities to promote the Chinese private sector. The Chinese government is focused on breeding digital giants in the e-economy. The DSR reinforces China's capacities to support emerging economies in their digital transformation, by adopting Chinese platforms and using these to their advantage, for example, by facilitating trade in remote areas.[183]

[180] Helm, T., "Pressure from Trump led to 5G ban, Britain tells Huawei", *The Guardian,* 18 July 2020, accessed 4 September 2021, at https://www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei

[181] The State Council, "The People's Republic of China", accessed 10 October 2021, at 中共中央 国务院印发《国家标准化发展纲要, 》

[182] Chipman Koty, A. "The China Standards 2035 Plan: Is it a follow-up to Made in China 2025?", China Briefing, accessed 30 September 2021, at https://www.china-briefing.com/news/what-is-china-standards-2035-plan-how-will-it-impact-emerging-technologies-what-is-link-made-in-china-2025-goals/.

[183] Dekker, B. and Okano-Heijmans, M., "Unpacking China's Digital Silk Road*", Clingendael Institute*, accessed 30 September 2021, at

Chinese corporations are supported through substantial government contracts, which allow them to invest heavily in research and development. Chinese companies are increasingly exporting surveillance technology such as advanced cameras and facial recognition, which help fledging authoritarian states to strengthen their control over society. In this way, Chinese digital exports are an *ideational* challenge, as well as an *economic* challenge.

Thus, the growing presence and influence of Chinese companies and the Chinese state in digital connectivity, combined with China's focus on digital sovereignty, pose economic, ethical and security challenges for Europe. At the same time, they complicate efforts to cooperate with China in the digital field. Responding to genuine needs in the market, Chinese technology giants are developing a strong presence in the European market and are early movers in developing countries and emerging economies, especially in South and Southeast Asia (China's backyard) but also in Africa, Central Asia and the Western Balkans (Europe's backyard).

Amid the US–Chinese tech rivalry, Europe must be more assertive in defending its own economic and strategic interests and promoting European norms. The EU and its member states must double down on efforts to develop players – that is, European technology giants and e-businesses – in the digital economy that will contribute to inclusive and sustainable growth at home and abroad, while also strengthening Europe's standard-setting power in the digital age.

Diverging approaches

Central to the debate and any policy decisions on digital connectivity are trade-offs concerning privacy, business interests and national security.[184] While all regulations are a balance of these three, the US has taken a path that prioritises the interests of businesses. This is most obvious in the strong focus on free data flows, both personal and non-personal, in order to strengthen companies' competitive advantage in collecting and using data to enrich themselves. China's approach, by contrast, strongly focuses on state security. Chinese businesses are supported and leveraged to pre-empt threats to the country and, more specifically, to the CCP. This is evident from its strict data localisation requirements to prevent any data from being stored beyond its borders, and a mandatory security assessment of cross-border transfers.[185] When combined with the

https://www.clingendael.org/sites/default/files/2020-07/Report_Digital_Silk_Road_July_2020.pdf.

[184] Dekker, B. and Okano-Heijmans, M., "Europe's Digital Decade? Navigating the global battle for digital supremacy", *Clingendael Institute*, accessed 1 September 2021, at https://www.clingendael.org/sites/default/files/2020-10/Report_Europes_digital_decade_October_2020.pdf.

[185] International Association of Privacy Professionals, "The future of data localization and cross-border transfer in China: A unified framework or a

expansive digital surveillance network that has been established in China, the authoritarian principles underlining Chinese digital policies are obvious.

The European Union represents a third way, emphasising individuals' privacy and a human-centred approach that puts people first and has a strong focus on ethics, including in data-protection regulations. This approach sets it apart from China, but its divergence with the US should also not be overlooked. The EU's regulatory actions have repeatedly brought it into conflict with US tech giants and a bilateral deal on data governance is set to be a key topic of Transatlantic debates and coordinated action on these issues, including in the EU-US Trade and Technology Council.[186]

It is evident that an autonomous digital policy is a key component of the push for "strategic autonomy" in Europe. The EU's prioritisation of democratic ideals and public privacy has pushed the bloc to establish policy programmes that guarantee a greater degree of technological and data sovereignty. Europe's divergence with China is less subtle. As outlined in the EU 2019 Strategic Outlook, Europe sees China as a partner, competitor and systemic rival.[187] The EU's divergence with China on digital policy is evidence of the systemic rivalry between the two powers, based on ideological beliefs which are ingrained in the design of digital systems. In addition, it is a competitor because Chinese companies and technology have become influential and successful in many markets, often at the expense of Western companies. However, the door has not been fully closed on China retaining its place as a valuable business partner for Europe.

The EU must continue to forge its own path on digital policy and work to build on the successes it has already had in exporting its standards, such as the global influence of the GDPR as a standard for data protection regulation. To do so, however, the EU must implement comprehensive and informed policy solutions that balance norms with economic competitiveness, and enhance cooperation in and with countries that share the EU's interests and values.

---

patchwork of requirements?", accessed 19 November 2021, at https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements/.

[186] European Commission, "EU-US Trade and Technology Council Inaugural Joint Statement", Press release, accessed 1 October 2021, at https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951.

[187] European Commission, "European Commission and HR/VP contribution to the European Council: EU-China, a strategic outlook", accessed 30 September 2021, at https://ec.europa.eu/info/sites/default/files/communication-eu-china-a-strategic-outlook.pdf.

Actionable steps

Digital connectivity efforts by the EU and its member states in third regions are largely shaped by policies in three, partly overlapping, domains: the digital agenda;[188] action on the Global Gateway;[189] and policies on priority regions, in particular the Indo-Pacific[190] and Africa.[191] Workable suggestions for future EU action will depend on a coordinated approach by the policymakers and stakeholders working in these fields. This will require a proper understanding of evolving policies in these three fields, which until now have largely been discussed separately.

The recommendations for future action below are grouped into four actionable steps that stand out as particularly promising for the EU in dealing with the digital China challenge: (a) move beyond being mainly a regulatory power; (b) focus on the Indo-Pacific and Africa; (c) invest in issue-based cooperation within networks; and (d) improve and expand digital development assistance and digital capacity building abroad, next to bilateral discussions between governments and multistakeholder discussions in international institutions. Each of these fields is rapidly evolving and a better understanding of the consequences of China's growing digital power is essential to any effective European response.

1. *Invest in market and standard-setting power*

The EU and its member states are slowly but steadily moving from being mainly a regulatory power to claiming their space as a player in the digital economy. The cloud computing initiative GAIA-X is a key example, as a proactive alternative to US and Chinese Cloud providers.[192] Such initiatives, including the more recent Next Generation Internet (NGI), are required to push European digital norms and standards, but also to boost the global competitiveness of European companies and business models.[193] Thus far, European companies have struggled to become as commercially successful as their US or Chinese counterparts and more support for the digital private sector may be warranted.

EU member states must also coordinate their engagement with international standard setting organisations and

[188] European Commission, "Europe's digital decade: the Digital Compass", accessed 30 September 2021, at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.
[189] European External Action Service, "Connecting Europe & Asia: the EU strategy", accessed 30 September 2021, at https://eeas.europa.eu/headquarters/headquarters-homepage/50699/connecting-europe-asia-eu-strategy_en.
[190] European Commission, "The Global Gateway", accessed 12 March 2021, at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6433.
[191] European Commission, "Africa-EU Partnership", accessed 15 September 2021, at https://ec.europa.eu/international-partnerships/topics/africa-eu-partnership_en.
[192] Gaia-X, "What is Gaia-X", accessed 15 September 2021, https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.
[193] Next Generation Internet, "The NGI Initiative: An internet of humans", accessed 14 September 2021, at *https://www.ngi.eu/about/*.

deepen their cooperation with European companies operating in the relevant sectors, to benefit from their technical expertise and understanding of the market. The contribution to standard developing organisations of Chinese governmental and private sector representatives has been growing since the 2000s. The Chinese government and Chinese companies used various means, such as direct subsidy of their participation and input, to expand their influence in international bodies and processes. Their primary focus has been on the organisations that have traditionally dominated the technology landscape, such as the ITU and ISO.[194] In addition to participation, they have shown great initiative in proposing standards. The presence and influence of Chinese actors in these standard setting bodies is likely to increase still further, putting increased competitive pressure on European technical industries and governments.[195] The EU needs to recognise and act on this new reality in the field of standardisation. This will require a better understanding of the implications for society and European economic competitiveness of the Chinese Outline for National Standardisation Development, which hinges on interdisciplinary research on the topic by Sinologists, technical experts and policy-oriented international relations experts. The EU will also need to strengthen its own multi-stakeholder approach to standard setting organisations.[196]

2. Prioritise the Indo-Pacific and the EU's African neighbourhod

Recognising the opportunities and disruptions that are accompanying the digital transition and green transformation globally, the EU and its member states need to increase their engagement with governmental, commercial and civil-society stakeholders and networks in the Indo-Pacific on a broad array of digitalisation issues.[197] The aim should be to establish mutually beneficial relationships, investments and exchanges in a region that is host to a vibrant digital ecosystem buoyed by booming e-commerce and FinTech applications, and the largest and most rapidly growing internet user base in the world.

Along with the Indo-Pacific,[198] the EU's neighbouring states in Africa, the

[194] Creemers, R. and Voo, J., "China's role in digital standards for emerging technologies: Impacts on the Netherlands and Europe",, Leiden Asia Centre, accessed 1 October 2021, at https://leidenasiacentre.nl/wp-content/uploads/2021/05/Chinas-Role-in-Digital-Standards-for-Emerging-Technologies-1.pdf

[195] Creemers, R. and Voo, J., "China's role in digital standards for emerging technologies: Impacts on the Netherlands and Europe", Leiden Asia Centre, accessed 1 October 2021, at https://leidenasiacentre.nl/wp-content/uploads/2021/05/Chinas-Role-in-Digital-Standards-for-Emerging-Technologies-1.pdf

[196] For a detailed discussion see the chapter on technical standardisation in this report.

[197] Okano-Heijmans, M., Nachiappan, K. and Dekker, B., "Fostering digital connectivity in and with the Indo-Pacific: Opportunities for the EU", European External Action Service, accessed 2 September 2021, at https://www.clingendael.org/sites/default/files/2021-04/Report_Digital_Connectivity_IndoPacific_April_2021.pdf.

[198] Okano-Heijmans, M. and Vosse, W., "Digital connectivity going global: the case for digital ODA", *Clingendael Institute*, accessed 2 September 2021, at https://www.clingendael.org/sites/default/files/2020-05/PB_The_case_for_digital_ODA_May_2020.pdf.

Western Balkans and Central Asia are crucially important to Europe's global interests and should remain a focal point of EU policy. Europe's "sister continent" was rightly explicitly labelled a priority area in the EU's Digital4Development policy by von der Leyen's European Commission. Africa has a staggering digital divide that the EU can work to bridge through digital connectivity policies that encourage inclusive, human-centred development. The EU must continue to build on its strong working relationship with the African Union, and ensure that digital policies are not overlooked as this relationship progresses. A useful next step will be to increase knowledge of the EU's digitalisation policies in the Indo-Pacific and Africa. Through research projects, the potential overlaps, convergences and divergences in the EU's digital efforts in these important regions can be compared and used to fine-tune the EU's digital policies.

3. *Develop issue-based cooperation networks and digital governance that puts people first*

Alongside "EU only" initiatives, working closely with partners that share the EU's concerns and interests will benefit the EU and its member states as they seek to fine-tune and implement their digital strategies. In addition to more traditional cooperation bilaterally and in international institutions, issue-based partnerships with (groups of) countries that share interests, concerns and values will continue to grow in importance. The US and specific Asian countries stand out as particularly promising partners. In the Indo-Pacific, networks could develop from existing cooperation with Japan, South Korea, the Association of Southeast Asian Nations (ASEAN) and three key players in the digital domain: India, Indonesia and Singapore. [199]

EU member states must also remain vocal in pushing for democratic ideals in international organisations. Many European concerns in relation to China's behaviour and increasing influence are shared by nations in other regions, including in Africa and the Indo–Pacific. European governments should engage more deeply with partners in these regions in order to form strong partnerships along new geographical lines. In addition to a more global outlook, these partnerships should pursue changes in emerging fields that will become increasingly prominent as the 21st century progresses.

4. *Digital Development Cooperation /Capacity Building*

The EU's 2017 Digital4Development policy has increased the prominence of digital solutions and technology in EU development policy.[200] The EU rightly recognises that digital technologies are proven enablers of sustainable and

[199] Okano-Heijmans, M., Nachiappan, K. and Dekker, B., "Fostering digital connectivity in and with the Indo-Pacific: Opportunities for the EU", European External Action Service, accessed 2 September 2021, at https://www.clingendael.org/sites/default/files/2021-04/Report_Digital_Connectivity_IndoPacific_April_2021.pdf.

[200] European Digital Development Alliance, "EU Digital4Development", accessed 15 September 2021, at https://europeandigital.org/policy/eu-digital4development.

inclusive growth. This policy framework has helped to mainstream the inclusion of digital development cooperation in European development policy, but the EU could do more to build the digital capacity of its international partners. The EU should take urgent action to end the dichotomy of a digital strategy that focuses on Asia and Digital4Development, which focuses on Africa.

The European Commission's 2030 Digital Compass has four core objectives: (a) creating digitally skilled citizens and highly skilled digital professionals; (b) secure, high-performance and sustainable digital infrastructures; (c) the digital transformation of business; and (d) the digitalisation of public services.[201] All four dimensions must be considered externally as well as internally, especially in developing countries and the emerging economies in Africa and the Indo-Pacific.

The EU must be more proactive in assisting third countries to establish data protection structures, fight cybercrime and facilitate e-commerce. Digital development cooperation and capacity building can be effective at launching long-term relationships, as the systems and hardware that the EU provides to partners will need maintenance and updates, which will encourage further cooperation and integration in the future.

Authors:
Brigitte Dekker is a PhD Candidate at Radboud University and an Associate Fellow at the Clingendael Institute in the Netherlands. Contact: bdekker@clingendael.org
Maaike Okano-Heijmans is a Senior Research Fellow at the Clingendael Institute in the Netherlands. Contact: mokano-heijmans@clingendael.org

[201] European Commission, "Europe's digital decade: the Digital Compass", accessed 30 September 2021, at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.


Digital Power China
A European research consortium