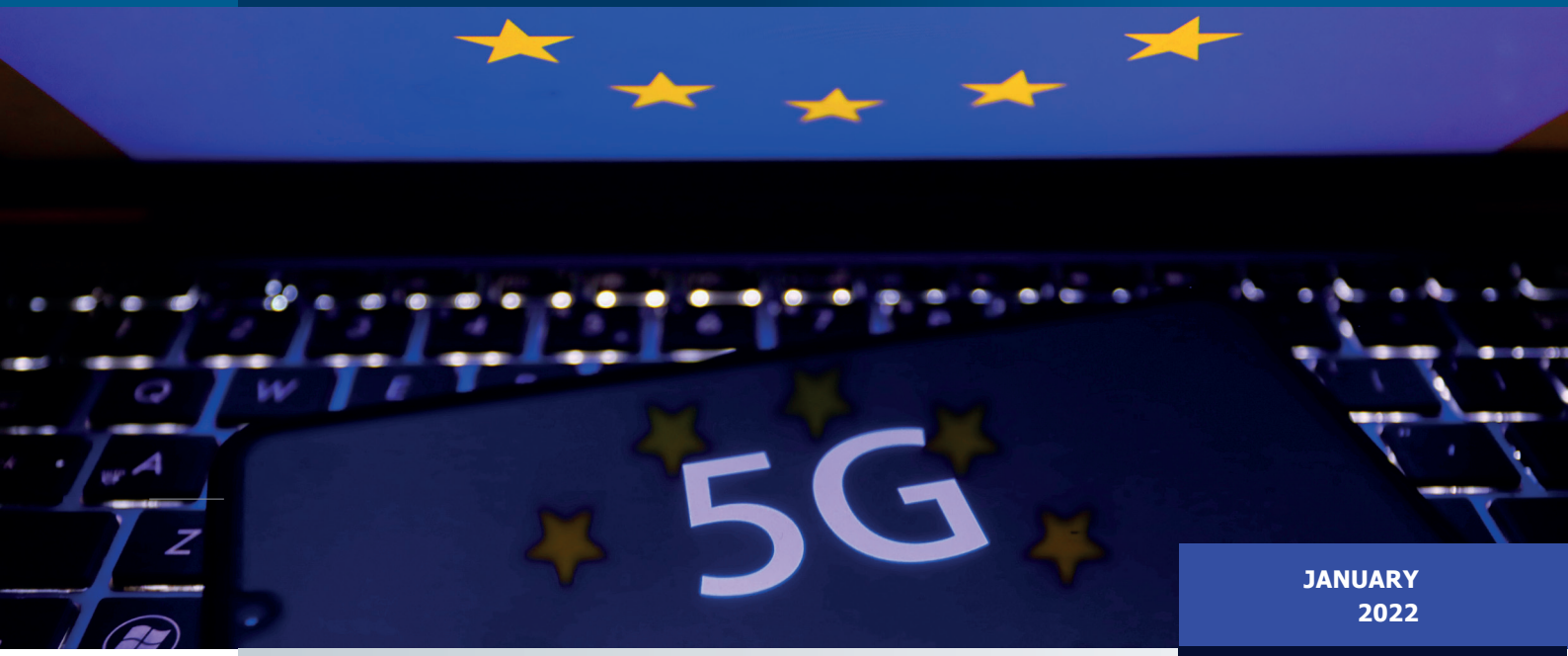
ÉTUDES
DE L'IFRI

GEOPOLITICS OF TECHNOLOGY PROGRAM



JANUARY
2022

Europe and the Geopolitics of 5G
Walking a Technological Tightrope

Julien NOCETTI

Ifri is France's leading independent think tank, promoting research, information, and debate on the subject of big international issues. Founded in 1979 by Thierry de Montbrial, Ifri is recognized as a public interest association (1901 law). It is not subject to any administrative supervision, has free rein over the scope of its activities, and regularly publishes the results of its research.

In the context of its research and debates, Ifri brings together an interdisciplinary team of policy makers and international experts.

Translated by Cadenza Academic Translations

ISBN: 979-10-373-0518-3

How to cite this publication:

Julien Nocetti, "Europe and the Geopolitics of 5G: Walking a Technological Tightrope", *Études de l'Ifri*, Ifri, January 2022.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

E-mail: accueil@ifri.org

Website: Ifri.org

Author

Julien Nocetti is an Associate Research Fellow at the French Institute of International Affairs (Ifri) and an Associate Professor at the Saint-Cyr Military Academy. He is also a member of the GEODE (Geopolitics of the Datasphere) center at the Université Paris 8, and heads the Cyber Risk Governance Chair at Rennes School of Business. Dr. Nocetti holds a PhD in Political Science and was a research fellow at Ifri for ten years up to September 2019. His research interests lie at the intersection between global politics and digital/cyber issues (geopolitics of data and artificial intelligence; cyber-conflict; tech platforms). He is also a specialist in Russia's foreign policy, in particular its digital and cyber strategies. He recently published "A Marriage of Consequence? Realities and Implications of the Russia-China Cooperation in Cyberspace" (*Études internationales*, Vol. 51, No. 2, 2021) and "Is Europe Still a 'Digital Colony' of the United States?" (*Politique étrangère*, Vol. 86, No. 4, 2021).

Executive summary

The acute Sino-American tensions which erupted in 2018 have been coupled with controversies around 5G technology, exemplified by the spotlight placed on the Chinese equipment manufacturer Huawei and the security risks associated with the use of their products and services. As in the case of artificial intelligence, 5G is a very sensitive geopolitical issue, raising concerns over the control of critical technologies. 5G is indeed critical, both since its use is expected to become quasi-ubiquitous, and owing to the gradual shift it entails toward network technologies based entirely on software, potentially strengthening already dominant players (digital platforms via cloud services).

For Europe, the issues surrounding 5G are painting a very complex landscape at the global level. Rivalry between the United States and China is limiting the European Union's room for maneuver, against a backdrop of security considerations and low levels of investment. The positions of the various actors on the continent (the European Commission, the main European powers, private firms such as Nokia and Ericsson) have not always been aligned, testament to an intricate web of technological dependencies on China and the United States. Meanwhile, the issue of semiconductors, symbolizing at once the EU's technological decline and the renewal of its ambitions, is integral to the development of 5G. They constitute the "musculature" of the system and trigger new geoeconomic challenges in which Europe has yet to find its place.

Contents

Introduction

On December 1, 2018, when the Canadian authorities arrested Meng Wanzhou—chief financial officer and daughter of the founder of the Chinese telecommunications giant Huawei—at the request of the United States, they had little inkling of the significant international tensions that were soon to come to a head prompted by the Sino-American technological rivalry.

The year that followed only served to confirm the stakes for Washington, Beijing, and beyond in terms of technological pre-eminence and the control of global supply chains. At the center of these tensions lay 5G—a technology of which Huawei is the world's largest supplier. At the time, the geopolitical importance given to the issue far outstripped the extent of its global deployment; indeed, 5G was only in its nascent stages at the time. 2019 was thus the year in which the issue of 5G became intensely "geopoliticized": a year in which the Trump administration levied various sanctions which not only curbed Huawei's international expansion and that of its subsidiaries, but also shook up the entire value chain underpinning the production of the semiconductors that are so essential for the functioning of 5G networks and ecosystems.

Two years on—and following the systemic crisis brought about by Covid-19—5G is still the subject of a series of paradoxes. The first is that this technology has managed to penetrate the realm of high politics even prior to its global dissemination. The point of difference in comparison with the internet is striking in this regard, and perhaps attributable to the acceleration of international conflict owing to the technological developments of the last decade. The second paradox is that most of the debates around 5G have so far focused on a single supplier (the Chinese Huawei), whose actions are largely dissected through the lens of Sino-American relations. For Europe, this distorting eyepiece conceals the risk of the continent getting caught in the metaphorical crossfire of China-US relations—dynamics which currently seem to form the main paradigm for a commercial, military, and technological understanding of the world.

Is 5G an additional challenge for a Europe already riddled with digital dependencies? Torn between a ready-to-go Chinese 5G offer (and the accompanying security risks) on the one hand, and pressure from the US to present a united front against China on the other, does Europe have the capacity to tread a hypothetical "third path", allowing it to avoid alienating Beijing, without necessarily aligning itself with

Washington? What is the best way to approach an issue that goes far beyond traditional telecommunications to encompass a myriad of issues, from matters of digital infrastructure (such as cables, data centers, and cloud architecture) to the proliferation of regulations and technical standards involved?

For the purposes of this article, discussion of 5G will be limited to the commercial sphere—5G military networks are certainly deserving of a separate and in-depth analysis.[1] This study looks at the two phases of the 5G rollout, each involving its own technological developments. The first phase, already underway, is known as non-standalone 5G and marks only a partial break with 4G. It deploys 5G radio alongside existing 4G core networks, multiplying the number of relay antennae in order to meet the challenge posed by higher frequencies.[2] Rollout of the second phase, or standalone 5G, is estimated to begin in 2023 (although timeframes differ from country to country), and it is at this point that we shall see a true paradigm shift in terms of telecommunication infrastructure. In addition to the mass distribution of relay antennae, software virtualization is expected to bring major developments in the field of health, agriculture, and the concept of Industry 4.0, as well as more generally, with the hyperconnectivity of the Internet of Things (IoT).[3]

1. In the field of defense, 5G networks together with artificial intelligence algorithms will connect soldiers, vehicles, and robots at high speed. 5G will also play a significant part in the battle network, owing to its capacity for connecting millions of transceivers within a circumscribed area.
2. In France, this fact poses a major constraint for operators, as the relay antennae must be made by the same manufacturer as the 4G equipment currently used by operators.
3. In other words, network infrastructures will no longer rely on fixed infrastructures but will in fact become modular and expandable. Significant investment is clearly necessary to achieve a complete standalone 5G network, since this requires entirely new platforms (particularly in the core network).

5G, a geopolitical challenge

5G completes the transformation whereby mobile connectivity has become a foundation infrastructure upon which many applications are developed. From a technological standpoint, it represents the culmination of a gradual transition to network technologies based entirely on software ("softwarization"). It also reinforces many doubts and uncertainties around the development of new technologies, such as their environmental impact, issues pertaining to security and cybersecurity, power games between various actors, and so on. For these reasons, 5G finds itself at the heart of renewed geopolitical controversies.

The issues around 5G… go beyond 5G

The technological angle: 5G as the future for the accelerated digitalization of our societies

Like artificial intelligence (AI)[4], 5G holds substantial promise, mainly defined in terms of growth drivers. Regularly referred to as revolutionary, the fifth generation of mobile communications overflows with new industrial, economic, and societal promise, relating to the hyperconnectivity of the IoT, IT systems, the development of smart cities,[5] connected agriculture, predictive financial and behavioral models, energy supply (smart meters, consumption forecasts, renewable energies), e-health (telemedicine and remote surgery), and even mobility, with autonomous vehicles

4. See J. Nocetti, "Intelligence artificielle et politique internationale. Les impacts d'une rupture technologique", *Études de l'Ifri*, Ifri, 2019, available at: www.ifri.org.

5. The term "smart city"—an intelligent or "hyperconnected" metropolis—refers to the use of technologies in urban areas to bring sustainable improvements to service quality and performance. Contexts include the optimal use of technologies—for public transport and green mobility, energy and water savings, recycling—and generally enhancing the economic and social qualities of the city. It is often confused with its security-focused counterpart, the "safe city", which, while still a hyperconnected environment, places the emphasis on using urban data and surveillance technologies ("smart" cameras and sensors) for public safety purposes.

representing the most widely popularized aspect of the foreseeable consequences of such networks.[6]

5G will initially function as an accelerator of existing digital trends, particularly as it can be deployed on existing bands and the current core 4G network. However, it paves the way for new disruptive services by offering innovative functionalities (such as its capacity for managing a large number of connected objects, ultra-reliable connection management, and differentiated network management in the form of virtualized "slices") and new frequency bands.

5G must also be considered in the broader context of the evolution of telecommunications, particularly the rollout of fiber with which it is inextricably linked. Furthermore, mobile telephony's advance toward 5G is accompanied by other technological innovations such as virtual reality and the advent of remote working.

More generally, the development of 5G has taken place alongside a veritable explosion in the amount of data produced and exploited worldwide. While the number of mobile phones in the world doubled between 2015 and 2020, the amount of digital data created annually increased from 33 zettabytes in 2018 to 64.2 zettabytes in 2020, with projections running to 180 zettabytes by 2025.[7]

Compared to 4G, 5G will operate on the basis of ecosystems that will interlink different domains, applications, and customers. This will be a largely virtualized ecosystem, centered around software rather than hardware infrastructures. It should be noted, however, that the 5G rollout does not rely on software advances alone: these networks will be accompanied by new hardware technologies, in particular new physical infrastructures to enable the transmission of larger amounts of data.[8]

Far more than a mere product of the evolution of a telecommunications standard, 5G can only be fully understood by considering it in all its complexity. Once more, like AI, it is akin to an extension of digital technology, amplifying its characteristics and shortcomings: the market is dominated by only a few actors, generating concerns around data collection and, more broadly, shifting technology's center of gravity toward Asia. Above all, 5G cannot be considered in isolation, or as in some way separate from its architecture: rather, it must be conceived of as a technological ecosystem, forming a continuum that spans the infrastructure itself,

6. For an overview of what is expected of 5G, see: "The 5G Era", McKinsey & Company, 2020, available at: www.mckinsey.com; E. D. Melo, A. Varas, H. T. Bernold, and X.n Gu, "5G Promises Massive Job and GDP Growth in the US", BCG, February 2, 2021, available at: www.bcg.com.
7. One zetta = 10^{21}. Data consulted by the author on www.statista.com.
8. On this subject, see J-P. Bienaimé's interview "Le déploiement de la 5G," in *Hermès, La Revue*, Vol. 85, No. 3, 2019, p. 149–154.

the cloud service, and data. Indeed, the virtualization of network functions leads to 5G merging with the cloud, resulting in a "5G cloud" of continuous data transmission to the end-user. Moreover, in conjunction with edge computing, 5G does away with the need for local communications to pass through a centralized infrastructure.[9] Lastly, AI chips are central to the rollout and smooth functioning of 5G, with this latter fueling increased demand for ever more sophisticated components.[10]

The systemic angle: Geopolitics and 5G

While clearly bound up with issues of economic competitiveness, 5G also has implications for political dependency and its associated risks, including blackmail, influence, and service outages. This represents one of the most striking features of the debate surrounding 5G so far: tensions are centered less on the actual technology, and more on the provenance of the original equipment manufacturers (OEMs)—particularly in the case of Huawei, the Chinese firm which is currently at the top of the leaderboard both in terms of technology and market share.

As a result, 5G has become the catalyst for renewed geoeconomic tensions and a marked Sino-American bipolarization, prompting a reshuffling of the major international players along with fresh diversification in the instruments available to countries for asserting their political power. 5G has thus triggered strong reactions even prior to its generalized international rollout.

Although Washington and Beijing have been engaged in an open trade conflict involving the imposition of tariffs on imported goods since January 2018, 5G has taken tensions between the two powers to a new geopolitical level. In May 2019, Donald Trump, who was president of the US at the time, banned Huawei from US 5G networks and announced sanctions that forced the company to overhaul its supply chains. All sales of American technology to Huawei—from semiconductors to mobile operating systems (such as Android)—were prohibited without official authorization.

9. "Edge computing" refers to computer processing that takes place in the immediate vicinity of the data source or user's physical location. Compared with the long journey otherwise made by such data to a server in the cloud, edge computing requires less bandwidth, enabling faster processing and decentralized organization. This means that data collected by IoT devices can be processed by the sensor or device itself, or by a local computer or server, rather than being transmitted to a data center.

10. W. Hettinga, "Semiconductor Test Volumes to be Driven by 5G, AI Chips", *eeNews Europe*, March 13, 2020, available at: www.eenewswireless.com.

A second presidential decree, signed at the same time, increased the scope of Trump's "technological decoupling" initiative. The US authorities were vested with the power to block the transfer of any technology that could see the critical infrastructure, digital economy, and national security of the US compromised by a "foreign adversary" (defined as a state, a company, or a natural person), even indirectly.[11] Although neither China nor Huawei were explicitly targeted, this measure is a major lever for controlling Chinese access to the American market, while remaining couched in sufficiently general terms as to enable its use for geopolitical purposes.

Beyond the national security risks invoked by Washington (using networks for espionage, infrastructure sabotage), US concerns also comprise a more symbolic aspect. Huawei—with its technological know-how, almost unlimited funds, and political support at the highest level—is perfectly poised to become the key player in the much-awaited 5G "revolution". This overturning of the course of digital history, thus far trailblazed by the US, represents a significant moment in the evolution of the international order: for the first time in modern history, a Chinese company is taking the lead in an advanced technology. The rationale underlying current competition between Beijing and Washington may be better explained by the "innovation imperative" than by any classic military rivalry[12] or trade dispute between the two countries.

The "geopoliticization" of 5G prompted by the Huawei case has laid bare the US's technological protectionism and fear of losing its technological superiority to Beijing. For two decades, the US has made data control the key axis of both its economic strategy, centered around its technology giants, and its security strategy. These two elements were visible for a long time in the American "open door policy", designed to open up markets and preserve American pre-eminence. Finding its apotheosis in Barack Obama's presidency, and later contested by Trump, this policy has mutated into the contemporary "weaponization of interdependence", whereby one's opponent can be weakened via the exploitation of economic ties previously forged with them.[13] With regard to the case in point, Sino-American technological interdependence has been greatly underestimated on both sides, as evidenced by the spotlight currently pointing at the highly globalized semiconductor industry,

11. "Securing the Information and Communications Technology and Services Supply Chain", US Department of Commerce, 2019, available at: www.federalregister.gov.
12. A. B. Kennedy and D. J. Lim, "The Innovation Imperative: Technology and US-China Rivalry in the Twenty-First Century", *International Affairs*, Vol. 94, No. 3, 2018, p. 553–572.
13. See D. W. Drezner, Henry Farrell, and Abraham L. Newman, *The Uses and Abuses of Weaponized Interdependence*, Washington DC: Brookings Institution Press, 2021.

held hostage by bilateral tensions at the risk of destabilizing supply chains and forcing restructuring or coalitions of interests.[14]

The convergence of national and geopolitical issues

5G illustrates the way in which, nowadays, global geopolitical issues are closely linked with national or even ultra-local issues. 5G is part of a wider "whole": it can scarcely be considered as separate from the ongoing technological changes and breakthroughs that are fueling fears over issues such as widening social and economic inequalities, job losses, and a desire for state control. The COVID-19 health crisis has accelerated this trend, and, in many regions of the world, contributed to anxieties around the use of technology for tracing and digital surveillance, reinforced by the power of digital platforms.15 The visibility of certain scaremongering content (videos, petitions, etc.) about the supposed implantation of electronic chips for geolocation purposes revives a genre of conspiracy theorizing that merely serves to blur public understanding of technological issues. 5G is sometimes viewed as a kind of externally imposed technological maelstrom (loosely encompassing AI, robotization, facial recognition), at the service of private interests.16

In a context where our relationship with technology represents a significantly divisive issue, 5G crystallizes deep-seated tensions around what actually constitutes progress. The "age of accelerations" that we are living in, and the dizzying amalgamation of technological advance, trade globalization, and climate change all challenge our capacity to understand and adapt, whether at the level of the individual, society, or economy.17 Illustrating perhaps that our democracies are out of step with technology, 5G could end up being rolled out only partially—in the case of intensified protests or radical actions against its installations (sabotage of antennae, etc.)—exacerbating the socioeconomic divide in Europe and accompanying feeling of distrust toward the elite.

14. See the third part of this study.
15. See O. Tesquet, *État d'urgence technologique. Comment l'économie de la surveillance tire parti de la pandémie*, Paris: Premier Parallèle, 2021.
16. For an analysis of the dissemination of conspiracy theories related to 5G in the context of the pandemic, see A. Bruns, S. Harrington, and E. Hurcombe, "'Corona? 5G? Or Both?': The Dynamics of COVID-19/5G Conspiracy Theories on Facebook", *Media International Australia*, Vol. 177, No. 1, 2020, p. 12–29; W. Ahmed, J. Downing, J. Vidal-Alaball, and F. López Seguí, "COVID-19 and the 5G Conspiracy Theory: Social Network Analysis of Twitter Data", *Journal of Medical Internet Research*, Vol. 22, No. 5, 2020.
17. T. L. Friedman, *Thank You for Being Late: An Optimist's Guide to Thriving in the Age of Accelerations*, New York: Farrar, Strauss & Giroux, 2016.

Technological coercion: The twofold effect of US sanctions

Now an inseparable component of US foreign policy, the use of sanctions rose heavily under Donald Trump, although the beginnings of a change in approach can be seen in Barack Obama's second term (2012–2016). External dealings are now more geoeconomic and unilateral in nature, and less concerned with any "negative externalities" that could befall Washington's main allies as a result.18

In the case of the sanctions decreed by the US administration against Huawei in 2019, the White House's about-face is twofold. On the one hand, these sanctions are not targeting a pariah state like North Korea or Venezuela; albeit indirectly, they are aimed at the world's second-largest economy, a member of the UN Security Council and a demographic giant. On the other hand, in addition to trade sanctions (the effect of which is not always satisfactory) and financial sanctions (which can have destabilizing consequences for the world economy), Washington has also deployed technological sanctions.

In the face of China's perceived technological ascendancy, this type of sanction relies on export control mechanisms intended to deprive Beijing (via Huawei) of access to the American market and therefore to domestic technological innovation and know-how, in particular in the semiconductor industry, where the Chinese authorities have undertaken a vast technological catch-up effort.

Known as "secondary" sanctions, they are purely extraterritorial and apply to all legal and natural persons, even those who have no territorial or personal ties with the US. They are not penal in nature, but are designed to heighten the impact of primary sanctions by presenting a choice to such actors as fall within their scope of application: a choice between severing their relations with any entities falling foul of the sanctions and therefore continuing to benefit from relations with the US, or maintaining such relations and accepting their total or partial exclusion from the American market.19

By denying access to the American market to Chinese companies and those whose products contain more than 25% American-made components, the Trump administration significantly curbed Huawei's international expansion and reminded the world that the US has considerable room for maneuver when it comes to global technology value chains. While this type of sanction undeniably equates to an ace

18. A Demarais, *How Sanctions Are Reshaping the World: A Journey Through the Global Ripple Effects of US Sanctions*, New York: Columbia University Press, forthcoming 2022.
19. P. Bonnecarrère (rapporteur), "Sur l'extraterritorialité des sanctions américaines", information report on behalf of the European Affairs Committee, French Senate, 2018, available at: www.senat.fr.

in the American sleeve in terms of exercising—and preserving—US power, it does not guarantee immunity from potentially negative consequences, not only for the US but also for its allies, along with companies and supply chains around the world.[20]

In this instance, while the sanctions have had no market impact in the US, they have, as intended, created significant constraints for Huawei vis-à-vis its procurement of semiconductors.[21] In May 2020, the Trump administration announced that it would ban all electronic component producers using American technology from manufacturing chips for Huawei, no matter where they were located. Three months later, the Department of Commerce strengthened the measures banning all sales of semiconductors to Huawei. By the end of the year, Washington had expanded restrictions to target dozens of other Chinese companies, including SMIC, China's largest electronics foundry. While similarities with financial sanctions exist, the difference here is that instead of targeting international companies using the dollar, the US has applied coercive measures to any company using American technology, irrespective of whether that company is American or foreign.

However, by putting Huawei in the international spotlight and weakening its expansionist ambitions, the US administration's actions have had the knock-on effect of strengthening Chinese actors under absolute state control. Thus, the public conglomerates Inspur and Datang experienced a significant upswing following US sanctions targeting Huawei, as did ZTE—a telecoms OEM with financial ties to the People's Liberation Army, and once subject to US sanctions.[22] The action taken by the US has moreover contributed to strengthening the perception that even the most globalized and Western-oriented Chinese companies cannot survive without the protection of the Party-state—an impression that Beijing is not in a hurry to dispel.[23] Lastly, the US sanctions are likely to have contributed to China strengthening its state-funded innovation capacities and accelerating its drive toward technological self-sufficiency.[24]

20. A Demarais, *How Sanctions Are Reshaping the World, op.cit.* For a pessimistic view on the utility of sanctions for the United States in the long term, see D. W. Drezner, "The United States of Sanctions: The Use and Abuse of Economic Coercion", *Foreign Affairs*, Vol. 100, No. 5, 2021, available at: www.foreignaffairs.com.
21. A. Capri, "China's Microchip Ambitions: Semiconductors Advance the Next Phase of Techno-Nationalism", Hinrich Foundation, 2021, available at: www.hinrichfoundation.com.
22. C. Balding, "ZTE's Ties to China's Military-Industrial Complex Run Deep", *Foreign Policy*, July 19, 2018, available at: foreignpolicy.com. In 2021, ZTE held around a third of the Chinese 5G market.
23. Interview with an expert, Paris, September 7, 2021.
24. B. Gill, "China's Quest for Greater Technological Self-Reliance," *Asia Society*, March 23, 2021, available at: asiasociety.org.

Europe: A testing ground for 5G

The various manifestations of 5G issues at the international level—as a technological battle and geopolitical backdrop, not to mention the omnipresence of American sanctions—mean that Europe is faced with an eminently complex landscape. The shadow cast by the Sino-American rivalry limits the European Union's scope for action, which is also conditioned by considerations pertaining to security and levels of investment. The positions of the various actors on the continent (the European Commission, the main European powers, private firms such as Nokia and Ericsson) have not always been aligned, testament to an intricate web of technological and political dependencies vis-à-vis the Sino-American duopoly.

The triple challenge posed by 5G for Europe

Security: Is 5G a critical infrastructure?

Owing to the generational leap that 5G represents for the future of companies and services that employ digital manufacturing, it can, along with energy infrastructure, be considered a critical infrastructure.

Just as with any new technology, 5G is not without its fair share of vulnerabilities and industrial risks. The latter are now mainly considered from the perspective of cybersecurity, since 5G is perceived to amplify exposure to cyber risk. Specifically, with 5G it is not possible to clearly differentiate the core from the edge of the network; as a result, it is more difficult to isolate certain components of the network compared with 4G. As explained by an IT security expert, "5G's dynamic software-based systems have far more traffic routing points. To be completely secure, all of these need to be monitored. Since this might prove difficult, any unsecured areas might compromise other parts of the network",[25] creating new vulnerabilities. The convergence and mutualization of networks present a risk related to the complexity of managing such a range of components (RAN, edge, core network, cloud, third-party applications) and ensuring they are fully secured in

25. "Is 5G Technology Dangerous? Pros And Cons of 5G Network", Kaspersky, www.kaspersky.co.uk.

the case of critical applications. As the number of lines of code increases, the network is ultimately left more vulnerable and harder to secure.[26]

In other words, unlike previous generations of telecommunications networks which relied mainly on hardware, 5G's "softwarization" enables it to be managed within a cloud environment, resulting in far greater potential exposure to attack. For example, the networks of an intelligent water supply system, if compromised, would leave the water open to deliberate contamination. Keeping 5G systems secure will moreover require permanent access to the networks and software, benefiting specialized technology firms while at the same time opening a window to less well-intentioned actors.[27]

Furthermore, the economic clout of the main operators is producing a quasi-oligopolistic market structure, with market power shifting from the US to China. Indeed, contrary to the situation seen during the 4G rollout, currently no American actor has mastered all the main components of 5G technology. The Chinese giant Huawei thus finds itself in a dominant position, leaving it free to shape international technical standards. Huawei's proven proximity to the Chinese authorities leads various Western democracies to question the wisdom of allowing the company access to their national infrastructures. Two major risks are associated with China in this context: that of developing a technological dependence on China likely to increase the risk of intrusion and cyberattack, and that of digital conflict ultimately manifesting itself as militarized offensive.[28]

Lastly, as reported by the EU's counter-terrorism coordinator, 5G stands to make it difficult for intelligence services to eavesdrop legally, owing to 5G's encryption of communications and its virtual and decentralized architecture.[29]

Sovereignty vs. interdependencies

For Europe, the debates surrounding 5G raise the question of how to balance global interdependencies with stated ambitions of sovereignty or strategic autonomy in technological matters. Issues of digital and technological sovereignty often come up in discussions around 5G. While digital sovereignty addresses a long list of fears (including loss of control over data, cybersecurity risks, digital rivalry in the provision

26. Exchanges between the author and technical experts, Paris, July and September 2019.
27. Interview with the author at the Agence nationale de la sécurité des systèmes d'information, Paris, November 30, 2021.
28. N. Inkster, *The Great Decoupling: China, America, and the Struggle for Technological Supremacy*, London: Hurst, 2020, p. 166.
29. Statement of Mr Gilles de Kerchove, Before the French Justice and Home Affairs Committee, 2020, available at: www.senat.fr.

of public services, threats to public freedoms and democratic values), technological sovereignty is additionally concerned with Europe's waning independence in terms of key technologies for strategic sectors (e.g., the defense industry and telecommunications structures, or—looking to the future—AI and the IoT).

Traditionally, we find two opposing readings when the issue of European technological sovereignty is raised. The first considers Europe as a vassal because of its lack of capacity for political and economic autonomy in this arena. The second believes in Europe's capacity for action regarding digital and critical technologies, citing high-level scientific expertise and the particular characteristics of a governance model grounded in European values.30 In reality, these two positions are not mutually exclusive: the EU knows how to leverage its technological excellence but stumbles over the geopolitically unprecedented nature of its political project, a fact which is sometimes crudely reflected in the international technological arena.

The most notable developments in 5G involve China. Previously motivated by the expansion of American "Big Tech", Europe's ambitions for technological sovereignty must now contend with China as well. This presents the EU with a number of new challenges, requiring it to rethink its position both on economic globalization, currently centered around Chinese productive capacity, and the "geopolitical" bent of the current Commission, as stated upon its inauguration in December 2019 at the height of transatlantic tensions. Europe's handling of 5G so far testifies to a lack of cohesion with Xi Jinping's China. The subject of varying opinion on the continent, the Sino-American rivalry nevertheless makes it difficult for Europeans to establish their commercial and strategic position with respect to China—and the US—given the rise in "technological nationalism" that Beijing is only too keen to export.31

Often relegated to the bench in political debates, the EU's capacity to act in the technological arena could be the be-all and end-all of an "on the move" strategy for 5G. This is a view that appears to be gaining traction in the Commission, which—aware of the EU's critical dependencies in strategic sectors—seeks to define measures to protect European interests. Indeed, the EU's "technological sovereignty" would be better defended by conducting a detailed assessment of Member States' critical dependencies and responding to these in a

30. J. Nocetti, "Is Europe a 'digital colony' of the United States?", *Politique étrangère*, Vol. 86, No. 3, 2021, p. 51–63.
31. N. Inkster, *The Great Decoupling, op.cit.*, p. 166. For a reading of techno-nationalism which contrasts political models, see G. Webster and J. Sherman, "The Fall and Rise of Techno-Globalism: Democracies Should Not Let the Dream of the Open Internet Die", *Foreign Affairs*, October 28, 2021, available at: www.foreignaffairs.com.

targeted way while remaining open to the rest of the world[32]—rather than adopting a classic approach to sovereignty, which ignores the fact that these interdependencies are a defining feature of the age we live in.[33]

Investment, R&D, and standards

A fundamental issue for Europe lies in the field of industry and investment. Debates around 5G have mainly focused on Chinese OEMs and concerns about the technology's potential impact on our health, leaving the important issue of competition between telecoms operators and major digital players to take a back seat. With regard to the former, the major challenge lies in monetizing the network enabled by 5G. In other words, the priority for telcos is to increase profitability for investors, as this has been damaged by GAFAM's disengagement from the necessary infrastructure works.[34]

5G is also contributing to the emergence of infrastructure funds, which are becoming central to the 5G ecosystem. Indeed, fund management companies are specializing in infrastructure investments, both as investors and operators. Some major European telcos have even gone as far as to sell part of their equipment and networks to these fund management companies in order to assuage their troubled balance sheets.[35] There has been a mushrooming of business entities dealing in the sale and rental of telecommunications equipment, and whose share capital is jointly held by a traditional telecoms player and a fund management company. Numerous partnerships between traditional operators such as Orange and Deutsche Telekom with US fund managers such as KKR, Carlyle, and Blackrock serve by way of example. More generally, the emergence of investment funds as key players in the financing of research, development, and production for all kinds of technical solutions illustrates that the race to 5G has left state actors standing on the sidelines. The independent American investment manager Neuberger Berman dedicated an entire portfolio to 5G in Europe in May 2020, after various funds dedicated to the Asian markets.[36]

32. D. Fiott and V. Theodosopoulos, "Sovereignty over Supply? The EU's Ability to Manage Critical Dependencies While Engaging with the World", *Brief No. 21*, European Union Institute for Security Studies, 2020, available at: www.iss.europa.eu.
33. On this subject, see P. Hérault, "Strengthening Sovereignty in the Era of Global Value Chains", *Études de l'Ifri*, Ifri, 2021, available at: www.ifri.org.
34. D. Boullier, "La 5G, un enjeu de rivalité majeur entre les opérateurs télécom et les GAFAM", *Le Monde*, May 28, 2021, www.lemonde.fr. This rift between telecom operators and GAFAM has been discussed in several interviews, and notably by the author in conversation with a European industrialist (Paris, June 8, 2021).
35. *Ibid.*
36. "Neuberger Berman 5G Connectivity Fund", *Funds Magazine*, October 30, 2020, fundsmagazine.optionfinance.fr.

Coming under the umbrella of research and development (R&D), 5G is, above all, a technology standard, encompassing a complex web of intellectual property rights. Standards help enable innovation, making it possible to achieve a key market share in critical technology. In terms of private actors, Chinese companies hold the strongest influence. Huawei holds the most families essential to 5G (1,554 as of March 2021) and is also the biggest contributor to the development of international technical standards.[37] China, on the other hand, seems dedicated to the search for an international consensus that would help it achieve greater market penetration, and has strengthened its participation in international standardization organizations accordingly (ISO and IEC in particular[38]).

The positions of European actors

Europe finds itself caught between tried-and-tested Chinese technology (albeit with all the associated security risks) on the one hand, and overbearing US diplomacy on the other, which seeks to unite its allies against China. Strikingly, the US even went as far as to pressure allies not to authorize Huawei's participation in the rollout of 5G networks on their territories (lobbying the UK, Germany, and France in particular). Within the EU, advances made by the various Member States appear relatively scattergun in approach, despite the fact that European technologies exist (Nokia and Ericsson).

Dispersion: The UK, Germany, and France

In Europe, it is the UK which has seen the most politicized debates around 5G and the use of Chinese technology. Westminster had initially decided to allow Huawei limited access to domestic 5G infrastructure. However, in July 2020, the UK government changed tack, imposing a blanket ban on the Chinese company entering UK markets, and resolving to eradicate any equipment already present in its networks by 2027. The first half of 2020 saw a major turning point in the bilateral relationship between London and Beijing. Within the UK, China was blamed for the development of the pandemic, owing to a lack of transparency over its handling of the crisis and its pressuring of the World Health Organization to avoid any global outrage against Chinese initial responsibilities in the pandemic. Furthermore, Beijing's aggressive diplomatic stance and its exploitation of "mask diplomacy"

37. J. McCormick, M. Bobrowksy, and D. Strumpf, "Huawei, Ericsson or Nokia? Apple or Samsung? US or China? Who's Winning the 5G Races", *The Wall Street Journal*, October 12, 2021, available at: www.wsj.com; T. Pohlmann and M. Buggenhagen, *Who Leads the 5G Patent Race November 2021?,* IPlytics, 2021, available at: www.iplytics.com.
38. Conversation between the author and a French industrialist at a standardization forum, Paris, November 23, 2021.

were viewed very negatively in London. The final straw came in the form of the national security law passed in Hong Kong on June 30, in violation of the Sino-British declaration of 1984.[39]

The decision nevertheless came as a surprise, as the UK had become central to the company's European strategy, with London home to its regional headquarters. In partnership with the British intelligence services, Huawei had also opened a Cybersecurity Evaluation Centre in 2010, to analyze and redress security vulnerabilities identified in its network. For some, this strategy was made possible thanks to a "skillful infiltration" of the country's decision-making structures, in particular involving shameless recourse to corrupt former leaders,[40] in reality a recruitment strategy aimed at ex-parliamentarians and members of ministerial cabinets,[41] something which is moreover fairly standard in Western countries.

The pressure exerted by American diplomacy, along with criticism of the British Conservative Party—within whose ranks had also formed a parliamentary group hostile to China—go some way to explaining an about-face that one British senior security official interprets primarily in geopolitical terms.[42] London subsequently turned to "Five Eyes" to find an alternative to Huawei,[43] either by bolstering the European companies Nokia and Ericsson, or by investing in open-source technologies. Lastly, the UK mobilized diplomatic action, consolidating a "coalition of democracies" known as the D-10 group (comprising the G7 countries plus India, South Korea, and Japan) designed to exclude Huawei from global technology value chains, and not just with regard to 5G.[44] Since the arrival of the Biden administration in the US, Westminster has been behaving in a less "theatrical" way, focusing its 5G initiatives on the diversification of its supply chains.[45]

39. J. Lunn, J. Curtis, and M. Ward, "The UK-China Relationship", *Briefing Paper,* No 9004, House of Commons, 2020, available at: commonslibrary.parliament.uk.
40. Conversation between the author and an employee of a British think tank, London, February 26, 2019.
41. See "Foreign Involvement in the Critical National Infrastructure: The Implications for National Security", Parliamentary report submitted by the Intelligence and Security Committee, London, 2013, p. 5–6, available at: assets.publishing.service.gov.uk; D. Sheppard, "John Browne: Oil Man Caught Up in Huawei Backlash", *The Financial Times*, July 18, 2020, available at: www.ft.com; R. Foyle Hunwick, "Britain's Conservatives Sold Out to Beijing Too Cheaply", *Foreign Policy*, May 20, 2020, available at: foreignpolicy.com.
42. Discussion at Ifri, Paris, July 20, 2021.
43. On the coordination of approaches within the Five Eyes alliance, see B. Seely, P. Varnish, and J. Hemmings, "Defending Our Data: Huawei, 5G and the Five Eyes", Henry Jackson Society, 2019, available at: henryjacksonsociety.org.
44. E. Brattberg and B. Judah, "Forget the G-7, Build the D-10", *Foreign Policy*, June 10, 2020, available at: foreignpolicy.com.
45. *5G Market Diversification and Wider Lessons for Critical and Emerging Technologies*, House of Commons Science and Technology Committee, February 2021, available at: publications.parliament.uk.

In Germany, divisions over the Huawei question in Angela Merkel's last government (2018–2021) have left Berlin's position unclear, and complicate German ambitions in terms of 5G and technological innovation. While the Social Democrats demanded Huawei's exclusion, on the basis that they suspected the Chinese operator of being subject to influence from Beijing, Angela Merkel feared offending China—Germany's largest trading partner—and falling behind in the rollout of 5G. The Christian Democrats were unable to find common ground, despite the Chancellor's proposal of a "third European way" involving the establishment of a certification agency for the creation of a common standard to assess and certify the various components of 5G.[46]

Pressure from national operators such as Deutsche Telekom (DT) to resume talks with Huawei came in the absence of any clear political direction, although the operator has stopped short of allowing the Chinese company to access its network cores. DT had imposed a moratorium on all commercial relations in January 2020, but ultimately competitive pressures became overwhelming, if the group was to compete in a market against competitors who continued to deal with the Chinese group—a situation complicated by the lack of a clear political signal.[47]

Germany remains the European power where the gap between clarity on the government's position and defense of industrial interests is most marked, "ultimately compromising European unity".[48] On the one hand, 5G's economic promise puts German car manufacturers in the line of retaliatory crossfire from both the Americans and the Chinese. On the other, political indecision over Chinese OEMs can be explained by a combination of several factors: naïve foreign policy (belief in China's respect for the rule of law and mutual non-espionage agreements), distrust of US objectives and reliability (potential Trump-Xi agreement), and the "mentality of controllable risks" peculiar to computer security actors, who had held greater influence in national debates up to early 2020.[49]

The new ruling coalition has not given a clear indication of the path it intends to follow for 5G, although its program mentioned the

46. On procrastination by the German authorities, see Y. Xu, "From IT Security Law 2.0 to Open RAN: Germany's 5G Strategy Evolves Beyond the Huawei Debate", American Institute for Contemporary German Studies, February 3, 2021, available at: www.aicgs.org.
47. N. Renaud, "L'Allemagne met 7 milliards sur la table pour accélérer dans la 5G", *Les Échos*, June 5, 2020, available at: www.lesechos.fr.
48. M. Huotari, "Im Zweifel auch mit weniger China", *Die Zeit*, June 29, 2020, available at: www.zeit.de.
49. Telephone interview with Stefan Heumann, Director of the Stiftung Neue Verantwortung (Berlin), March 4, 2021.

creation of a "5G and 6G open-source consortium" (see below) and a desire to guard against "extraterritorial sanctions".

In France, the "anti-Huawei law" (as dubbed in the media) was adopted by Parliament in July 2019. It aims to "protect French defense and national security interests in the context of the operation of mobile radio networks".[50] An authorization scheme will allow operators to use 5G equipment under licenses of three to eight years. While the law does not mention Huawei and ZTE directly, the potential for interference by these actors and the risk this poses for the national interest are carefully evaluated. Rarely stated explicitly, the French stance seeks to discourage French operators from using the Chinese firm for 5G, while avoiding banning it altogether. The Chinese company will, in principle, be able to participate in the future deployment of 5G equipment but will be unable to access the core mobile network. Sites deemed sensitive or strategic—such as the Paris region, Brest, Marseille, Rennes, and Strasbourg—will also be off-limits. This implicit desire to exclude Huawei has been a cause for concern for French operators since 2019: the Chinese giant already supplies about 50% of Bouygues Telecom and SFR's 4G network equipment. In the summer of 2020, Bouygues Telecom announced that they would phase out 3,000 Huawei-made relay antennae deployed in densely populated areas by 2028.[51] Orange and Free have turned to Nokia and Ericsson, but nevertheless fear that Huawei's exclusion could cause a price hike due to the latter's privileged market position.

Just like the UK, France has had Huawei on its watch list for some time now: in the conclusions to his 2012 report, Senator Jean-Marie Bockel warned of the risk posed by the Chinese OEM to French technological sovereignty, given the advantage it had derived over the preceding decade from the French company Alcaltel's activities in China.[52] At the national level, 5G is more the subject of political division than informed public debate.[53] Lastly, along with the UK and Germany, France has found itself the subject of various threats issued by the Trump administration should it decide to authorize Huawei's participation in the deployment of future national networks. Indeed, in 2019–2020, the Franco-American diplomatic agenda was punctuated by blackmail over intelligence sharing, retaliatory trade sanctions, and the drawing of a link between France's position on Chinese 5G and the

50. J. Lausson, "Le Parlement valide la loi sur la sécurité de la 5G : et maintenant ?" *Numerama*, July 4, 2019, available at: www.numerama.com. The text of the law is available at: www.legifrance.gouv.fr.
51. M. Rosemain, "Bouygues to Remove 3,000 Huawei Mobile Antennas in France by 2028", *Reuters*, August 27, 2020, available at: www.reuters.com.
52. J-M. Bockel (rapporteur), "La cyberdéfense, un enjeu mondial, une priorité nationale", information report made on behalf of the Committee on Foreign Affairs, Defense and Armed Forces, French Senate, 2012, available at: www.senat.fr.
53. M. Darame, "La classe politique divisée sur la 5G", *Le Monde*, September 25, 2020.

US's respect for military alliances. As a corollary to the intransigence of the former Trump administration, Huawei increased the intensity of its overtures to French politicians.[54]

The European Union: An incomplete toolbox?

These examples from the three main European powers clearly show the difficulty experienced by these countries in trying to strike a balance between economic competitiveness and associated security risks. But they also testify to European indecision regarding Xi Jinping's China—perhaps the most revealing aspect of the tensions around 5G.

The European Commission spoke out only timidly and belatedly on the issue of 5G. In January 2020, the launch of a 5G "toolbox" in part came to redress the balance. Although it does not name China directly, the document implies in veiled terms that Chinese operators are "high-risk suppliers", leaving Member States to take their own decisions over who to partner with internationally for the provision of infrastructures.[55] Indeed, each Member State remains free to decide its own strategy, leading to significant disparities between countries. The European Commission additionally recommends that operators use several suppliers, in order to reduce dependence on any particular one and thus lower the associated risk. This essentially has the effect of limiting Huawei's market share within the EU and confirms Brussels' delicate handling of the issue, in the aim of achieving "appropriate and proportional" measures.[56] A more critical reading might suggest that the EU would have been better advised to approach its 5G policy from an industrial policy perspective, rather than in terms of national security, as this latter constitutes an area in which the Member States are sovereign.

Lastly, the Commission has to contend with the diplomatic pressure exerted by the US: apart from the three member countries mentioned above, others have also taken measures to prevent telcos from using Chinese equipment for 5G. Sweden, Latvia, and Estonia are notable examples, along with the Clean Network Program signed by Bulgaria, Romania, Slovakia, and Greece with the US. In general, Eastern Europe—a sub-market favored by Chinese OEMs[57]—has been the subject of sustained diplomatic efforts by the US: three "Prague

54. S. de Royer et Nathalie Guibert, "L'intense lobbying du géant chinois Huawei auprès des décideurs politiques français", *Le Monde*, March 3, 2021, available at: www.lemonde.fr.
55. The text of the "5G Toolbox" is available at: digital-strategy.ec.europa.eu.
56. D. Danet, S. Taillat, and J. Nocetti, "EU Cyber Defense", *EU Policy Brief*, No. 3, Center for European Studies, Carleton University, 2020, p. 2, available at: https://carleton.ca.
57. F. Jirouš and J. Lulu, "Huawei in Central and Eastern Europe: From Strategic Partner to Potential Threat", *e-International Relations*, May 19, 2019, available at: www.e-ir.info.

conferences on 5G security" have been held since 2019 in the Czech capital, with the support of the White House.[58] These efforts are aimed at ensuring that the security risk associated with the rollout of 5G is kept firmly on the agenda, along with the need for a common position (i.e., similar to that of the US) vis-à-vis China.

Nokia and Ericsson: The emancipation of the European leaders

Unlike the Swedish company Ericsson, which does not yet offer optical transmission or routing, and is thus forced into commercial partnerships in order to provide a complete service, Finland's Nokia is the only player—apart from Huawei—to dominate the entire spectrum of 5G technology from network access to transport, via traffic aggregation, optical transmission, switching, routing, and even access to submarine cables.

Support for domestic OEMs, however, reveals differences between China and Europe. Beijing's well-documented political and financial support for Huawei is quite different from the support that Nokia and Ericsson receive from the European institutions. While the geopolitical context has enhanced Brussels' benevolence toward these two actors, they still have to abide by the dictates of the liberal economy, including respect for the rules of free competition, unlike their Chinese counterparts. Indeed, Nokia and Ericsson remain competitors in terms of technological development, patents filed, and contributions to the 3GPP standard.[59] This intra-European competition does not appear to be negatively viewed by the executives of these companies, who seem more concerned about delays in Europe's rollout of 5G technology.[60]

Moreover, the EU has the advantage of being home to two large 5G infrastructure companies, Nokia and Ericsson, whereas the US lacks such giants in the current configuration where the closed proprietary model remains dominant. In 2020, Huawei controlled 29% of the global mobile base station market, and is now, by far, the company to offer the most advanced equipment.[61]

58. "Statement by NSC Spokesperson Emily Horne on US Support for the Third Annual Prague 5G Security Conference", The White House, December 2, 2021, available at: www.whitehouse.gov.

59. The 3GPP, or "3rd Generation Partnership Project", brings together seven telecommunications standards organizations, and produces and publishes technical specifications for 3rd, 4th, and 5th generation mobile networks.

60. See the interview with Ericsson's CEO in *Le Monde*, April 17, 2021, available at: www.lemonde.fr.

61. In the same year, market share for Huawei's main competitors stood at 26% for Ericsson, 21.5% for Nokia, and 9% for Samsung. Source: Trendforce, 2021, available at: www.trendforce.com.

At the height of the Sino-American tensions, some senior American officials had publicly suggested the idea of the US government buying a controlling stake in the two European companies, before the vice-presidency swiftly moved to deny the proposal.[62] The idea reappeared in the summer of 2020, this time via rumors that it would be the US OEM, Cisco, to buy majority shares in the two European companies.[63] Like any economic player however, Nokia and Ericsson remain vulnerable to US sanctions. In December 2019, Ericsson paid one billion US dollars to the Treasury to settle corruption charges brought by the US Department of Justice, who accused the company of bribing government officials in five countries—including China.[64] In its annual report for the same year, Nokia announced it would no longer be taking on any new business in Iran, citing the lack of a common regulatory framework between the EU and the US.[65] In September 2021, the company also had to put its technical collaboration with the O-RAN Alliance on hold (see below), for fear of facing secondary sanctions from the US owing to participation in the alliance by various Chinese companies who were included on the US Department of Commerce's "entity list".[66]

The weighing of such geopolitical risk is also mirrored in China, where the two European OEMs now only win very minor contracts, with Beijing awarding almost all tenders to Huawei to ensure the domestic company receives financial backing.[67]

Ericsson and Nokia are nevertheless taking advantage of Huawei's fall from grace on the continent to consolidate their European market share, with the three holding 31%, 28%, and 26% of the market respectively in 2020.[68] In the same year, Huawei reportedly lost 40 contracts in Europe, principally to Ericsson's benefit.

Support from the European authorities is unwavering, both in word and in deed. In his 2020 speech, Commissioner Thierry Breton drew a connection between use of the European operators Nokia and Ericsson, and the issue of Europe's technological sovereignty.[69] With

62. D. Shepardson, "White House Dismisses Idea of U.S. Buying Nokia, Ericsson to Challenge Huawei", *Reuters*, February 7, 2020, available at: www.reuters.com.
63. D. Fitzgerald and S. Krouse, "White House Considers Broad Federal Intervention to Secure 5G Future", *The Wall Street Journal*, June 25, 2020, available at: www.wsj.com.
64. "Ericsson Agrees to Pay Over $1 Billion to Resolve FCPA Case", The United States Department of Justice, December 6, 2019, available at: www.justice.gov.
65. Reuters Staff, "Nokia Says It Is Not Taking on New Business in Iran", *Reuters*, March 21, 2019, available at: www.reuters.com.
66. R. Le Maistre, "Nokia Gets Back on the O-RAN Alliance Track", *Telecom TV*, September 14, 2021, available at: www.telecomtv.com.
67. P. Boutin, "China Mobile Excludes Ericsson and Nokia From its 5G Development", *Mobile World Live*, October 5, 2021, available at: www.mobileworldlive.com.
68. "Wireless Infrastructure Report", LightCounting, February 25, 2020.
69. T. Breton, "Speech by Commissioner Thierry Breton for the Digital Life Design (DLD) Conference in Munich", Munich, January 20, 2020, available at: www.youtube.com.

regard to more tangible advocacy, the EU has partnered the two companies in its Hexa-X research project to shape the 6G of the future by 2030.[70]

OpenRAN: Pros and cons

As we have seen, 5G will rely on cloud computing to exploit significant volumes of data. Managing this data—in particular that pertaining to industry—along with their means of access, constitutes a fundamental issue in terms of autonomous economic and political decision-making. This risk of dependency is nothing new. Currently, Huawei, Ericsson, and Nokia together account for 80% of the European telecommunications network infrastructure market. Banning Huawei from the 5G rollout would create a duopoly dominated by Ericsson and Nokia in a market which is already oligopolistic.

The O-RAN (Open Radio Access Network) initiative proposes a direction that is acquiring significant international visibility, in the form of an international consortium comprising a large number of American, Chinese, and European operators (including AT&T, China Mobile, Deutsche Telekom, NTT DoCoMo and Orange), aimed at decoupling the radio part from network optimization and control software. The advantage of such segmentation, based on OpenRAN technology, lies in identifying specific functionalities and sectors (such as electronics, physical layers, antennae, and signal processing on the one hand, and algorithmic resource sharing and software on the other) that can be designed and programmed independently, in particular using open-source software.

In other words, the project is aimed at developing a 5G network by using open interfaces. The idea is to split the 5G network into small areas (a practice known as “network slicing”) whose standardized architecture would enable new players to offer their services. In addition to the initial aim of facilitating competition and thus avoiding the formation of oligopolies, the diversification of suppliers also mitigates risk and is thus viewed favorably by the European Commission in particular.

One of the advantages for operators is that of being able to use equipment from different manufacturers. As this approach involves the creation of a new interface however, it could potentially involve slower data transmission. In addition, the responsibility for end-to-end time guarantees would be shared between two different entities.[71] Unanimous agreement therefore does not exist regarding its adoption.

70. See the Hexa-X project website: https://hexa-x.eu.
71. Telephone interview conducted by the author with a French OpenRAN expert, December 15, 2021.

Three further risks of a different nature are also cited in connection with OpenRAN. The first is to do with securing the technology. Public access to open-source code—vulnerabilities included—is, first of all, an inherent weakness of free software. A sharp increase in cyber-incidents has been seen in applications on servers running Linux, which makes them prime targets for hackers acting on behalf of state services.[72] This parameter is interpreted in various ways: for some, OpenRAN's expected benefits outweigh this vulnerability, which they claim has been exaggerated. For others, OpenRAN takes a risk specific to one operator, Huawei, and turns it into a quasi-systemic one owing to the nature of open-source software[73]. The presence of Chinese actors in the O-RAN Alliance (representing a total of 44 out of the 237 mobile operators and network equipment providers) can also be perceived as something of a political inconsistency on the part of the West, since they will evidently have access to the code and intellectual property pooled regardless.[74]

The second risk concerns Europe's place in the international standards game. Indeed, Sino-American tensions could eventually lead to a collapse in the prevailing consensus on the standardization established by the 3GPP and the Internet Engineering Task Force in these areas, which could significantly alter the landscape. Influence remains a key consideration in bodies where the stakes have taken on a geopolitical hue: paradoxically, the 3GPP is thus deemed to "highlight certain specificities [of OpenRAN] which could replace the existing global specificities".[75] The risk here is that Europe witnesses a fragmentation of standards along geographical lines which stands to weaken—if not render entirely impossible—their interoperability.

Lastly, OpenRAN is a welcome gateway for leading cloud service providers worldwide—namely, Amazon Web Services, Google Cloud, and Microsoft Azure—that would capture the value generated by cellular networks. These three GAFAM companies have established themselves in the telecommunications sector by constituting a "technical base" for operators. By squeezing traditional manufacturers and operators, they expect reduced costs and thus weigh in on the ongoing upheaval affecting future 5G value chains, in keeping with the US policy of "technological decoupling". These companies have therefore multiplied contracts with operators: Google has partnered

72. E. Chickowski, "Next-Gen Supply Chain Attacks Surge 430%", *DarkReading*, August 21, 2020, available at: www.darkreading.com.

73. Conversation between the author and a Google France manager, Paris, September 13, 2021; telephone interview conducted by the author with an Orange technical executive, November 26, 2021.

74. Email exchanges with Thorsten Benner, Director of the Global Public Policy Institute (Berlin), November–December 2020.

75. Conversation between the author and a French industrialist at a standardization forum, Paris, November 23, 2021.

with Orange, Telefonica, Vodafone, and Telecom Italia, in addition to a collaboration with Ericsson to provide companies with private 5G networks. Microsoft has struck a deal with AT&T, and AWS counts Bell, Swisscom, and Verizon among its partners. Facebook has also joined the O-RAN Alliance and is partnering with the American microchip manufacturer Marvell in the development of its own 5G infrastructure (the "Evenstar"[76] project).

It should also be noted that OpenRAN is becoming a common theme in international relations. Much loved by US diplomacy which sees it as a means of boosting domestic strengths in terms of software and the cloud, OpenRAN thus revives a conflict of values between those in favor of the opening up of networks, and the proprietary model preferred by Huawei, Ericsson, and Nokia. Here, it is worth thinking about OpenRAN less in terms of its technological and economic added value, and more in terms of its utility to the US in consolidating a social imaginary around the notion of freedom in the context of the Sino-American rivalry.[77]

76. J. Morra, "Marvell Partners with Facebook to Build Open 5G Base Stations", *Electronic Design*, March 4, 2021, available at: www.electronicdesign.com.
77. J.-C. Plantin, "The Geopolitical Hijacking of Open Networking: The Case of Open RAN", *The European Journal of Communication*, Vol. 36, No. 4, 2021, p. 404–417.

Semiconductors: At the heart of 5G in Europe

The battle for investment, security, and technological prestige relating to 5G goes beyond the matter of 5G technology and Chinese manufacturers. Closely linked to the technical and commercial development of 5G, the semiconductor issue is—for Europe as for the US and China—not merely a tangential issue: it lies right at the very heart of what is at stake, with Europe's capacity to master its interdependencies determining its strategic and economic future.

The mother of all technological battles

Semiconductors have long played a supporting role in the technological rivalry and trade tensions between China and the US. This is due to various factors: technological competition (the integrated circuits and processors used in AI are more and more sophisticated and miniaturized); their economic significance (demand for them is growing exponentially and they constitute a highly globalized industry) and their strategic aspect (they are dual technologies).

Over the past three years, the industrial aspect has become closely intertwined with its geopolitical counterpart: China continues its push for self-sufficiency and technological catch-up relative to advanced semiconductors, which are currently the weak link in its innovation-oriented development strategy. Beijing's aspirations in this arena have never translated into any degree of leadership, despite the "531 Plan" launched in 1986, or the 50 billion US dollars allocated to integrated circuits in 2014. Chinese manufacturers lack expertise and a sufficiently strong industrial base in this sector, in particular regarding the most sophisticated components, making chips the country's number one import, ahead of hydrocarbons.[78] The geopolitical factor is limiting China's ability to catch up in the short term, with the country banking on its advances in the realm of AI to make up for the delay.

For its part, the US wants to reshape the industry's global value chains and develop greater control over critical components for its digital weapons. Donald Trump sought to hinder Beijing's quest for

78. A. Capri, "China's Microchip Ambitions: Semiconductors Advance the Next Phase of Techno-Nationalism", Hinrich Foundation, 2021, available at: www.hinrichfoundation.com.

technological independence, a move which also penalized some American and allied (Taiwanese, South Korean, and European) manufacturers and developers. Current trends are aptly illustrated by the example of the Taiwanese company TSMC, a leading manufacturer of semiconductors (responsible for 54% of world production in 2020[79]).[80] Huawei—operating through the Chinese foundry SMIC—does not possess complete mastery of the necessary production know-how for the most sophisticated chips, and is thus dependent on the renegade island firm. Following Donald Trump's May 2020 sanctions aimed at hindering China's supply, TSMC stopped exporting to Huawei. To make up for the resulting shortfall in TSMC's turnover, the US encouraged the company to open a production site in Arizona, offering fiscal advantages in order to facilitate its doing so. The crisis merely confirms the inevitability of TSMC's pre-eminence—this is a company whose technological superiority permits it to contemplate investments of tens of billions of dollars in R&D and new industrial sites.[81]

Joe Biden's inauguration prompted the new administration to conduct a detailed assessment of its supply chain. The exhaustive report on AI published by the Commission in March 2021 seems to indicate that, for the US, competition with China over AI is closely bound up with mastery of the technology involved in the manufacturing of semiconductors and the capacity to produce their component parts on American soil.[82]

Europe: Avoiding technological predation

As with software and digital platforms, Europe has relatively little clout in this strategic industry. Players of any significant size are few and far between: the Swiss company STMicroelectronics (previously under Italian management), Germany's Infineon, and the Dutch NXP ranked 12th, 13th, and 14th respectively on the global industry leader board by revenue in 2019.[83]

Europe—and France by extension—has chosen to focus on R&D and design in this sector, at the expense of component production. Indeed, less than 6% of the world's semiconductors are currently

79. TrendForce, August 31, 2021, available at: www.trendforce.com.
80. TSMC is a foundry: it manufactures semiconductor devices but is not responsible for designing them.
81. P. Escande, "L'histoire de l'entreprise taïwanaise TSMC est celle de la mondialisation… et de ses limites", *Le Monde*, October 14, 2021, available at: www.lemonde.fr.
82. *National Security Commission on Artificial Intelligence*, March 2021, available at: www.nscai.gov.
83. Data compiled *via* Anysilicon, available at: anysilicon.com.

produced here. This situation was first brought to the French Senate's attention back in 2008: the fact that Europe is choosing to specialize in circuit design over the production of components "will eventually lead to the disappearance of the European microelectronics industry and ensuing loss of global competitiveness for whole swathes of the economy".[84]

Technologically speaking, Europe cannot compete when it comes to the ultrafine etching of circuit boards (3–5 nanometers). The Dutch company ASML however has made a ground-breaking advance in this area: it manufactures not chips, but lithography machines, which play a vital role in the process of printing semiconductors by exposing them to UV light. This is what makes the fabrication of ultra-miniature chips possible. It is also the reason why the company came under immense pressure from the Trump administration in 2020 to cancel a contract with China.

ARM, a British company bought by the Japanese fund Softbank, also features among these coveted European nuggets. The company's particularity revolves around a standard upon which nearly the entire industry depends for designing their chips. ARM architecture is an instruction set enriched by client contributions. Embodying the "fabless" approach taken by the majority of Western players, which sees the outsourcing of production to enable an exclusive focus on design, ARM has been embroiled in a takeover bid by the American chip designer Nvidia for 40 billion euros since 2020. Qualcomm and Samsung were among those raising concerns over the implications for competition, prompting the US regulatory body to oppose the bid in December 2021 on the grounds that the resulting company would leave all its rivals with no choice but to do business with it. In 2021, the European Commission launched an investigation on the same grounds, as did the UK regulator, which further cited national security concerns.

China is, unsurprisingly, interested in the European semiconductor industry, and has been multiplying its acquisitions on the continent via investment funds. Attempts to buy out a French company failed in 2021, but the past two years have seen German and Austrian companies sold off to funds serving as a front for Chinese interests.[85]

84. Claude Saunier (rapporteur), "L'industrie de la microélectronique : reprendre l'offensive", Report made on behalf of the Parliamentary Office for the Evaluation of Scientific And Technological Options, French Senate, June 2008, available at: www.senat.fr.
85. J. Bouissou, "Semi-conducteurs: la Chine multiplie les achats en Europe", *Le Monde*, November 3, 2021.

The Chips Act and the search for partnerships beyond Europe

Against a still volatile geopolitical backdrop, marked by the worldwide shortage of components, the predatory pressures exerted on the European semiconductor industry have prompted the Commission to take more substantial measures than those previously envisaged by the "2030 Digital Compass" published in March 2021. Proposed in the first quarter of 2022, the Chips Act established the goal of doubling European chip production capacity by 2030. To this end, the Commission launched the Industrial Alliance on Processors and Semiconductor Technologies in July 2021—an initiative aimed at identifying and remedying the EU's dependencies in this arena, so as to increase its market share of global production to 20% by the end of the decade.[86] Rooted in the desire to build a European sector as part of an Important Project of Common European Interest, this ambition furthers the discussion around European "technological sovereignty", which also encompasses cloud services and low-orbit satellite networks. It moreover entails the participation of world-class research laboratories such as the Interuniversity Microelectronics Centre in Leuven, the CEA-LETI in Grenoble, and the Fraunhofer Institute in Munich.

Delving below the headlines, we would highlight, on the one hand, the conspicuous absence of any link between the EU's pronouncements on semiconductors and the issue of 5G, despite the fact that the explosion of connectivity underlying the development of 5G will increase the demand for electronic components.[87]

On the other hand, the movement to secure supply chains also relates to Europe's place in its global technological environment. The Chinese issue was still the main obstacle to an agreement between American and European executives on the subject of semiconductors at the EU–US Trade and Technology Council in September 2021, forming the subject of an almost doctrinal obsession on the American side, and illustrating the discrepancy between political discourse and commercial reality on the European side.

86. "Digital Sovereignty: Commission Kick-Starts Alliances for Semiconductors and Industrial Cloud Technologies", European Commission, July 19, 2021, available at: ec.europa.eu. Among the projects launched was the construction of a semiconductor foundry in partnership with Intel and TSMC.
87. L. Cameron, "As 5G Approaches, Semiconductor Industry Must Combat Friction Points to Make World of 'Smart Everything' A Reality", IEEE Computer Society, available at: www.computer.org

The relocation of production is posing a major transatlantic challenge. The three largest chip producers, TSMC, Samsung, and Intel, have all announced substantial investments in new production sites located in the US. The future of transatlantic relations will partly play out in this geoeconomic arena.

Ultimately, given TSMC's technological lead, Taiwan is central to this industry, and thus finds itself courted by major global technology actors who want to attract this company to their territory. While the US and Japan may have been first to leave their calling card, Germany is currently in discussions over the construction of a plant.[88]

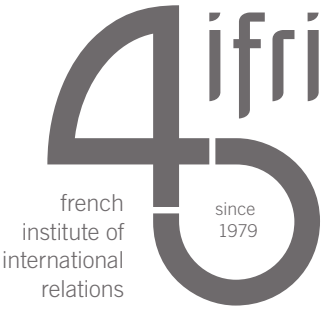
88. D. Wu, "TSMC in Early-Stage Contact with Germany about Potential Plant", *Bloomberg*, December 11, 2021, available at: www.bloomberg.com.

Conclusion

Representing the potential to exploit and share data with a speed, responsiveness, and ease-of-use which have never been seen before, 5G—at least in its standalone guise—nevertheless constitutes a step into the unknown in terms of the risks associated with its technology. From a geopolitical point of view, 5G is the "product" of two sequences of events. The first involved the polarization of international debate which accompanied the cooling of Sino-American relations over the Huawei affair, setting in motion the "decoupling" of the two countries' technological ecosystems—the outcome of which remains uncertain as long as existing interdependencies persist.

The second pertains to the impact of the global health crisis, which exposed the general public to the phenomenal scope and importance of supply chains, not to mention their vulnerability. From a corporate standpoint, the proliferation of economic sanction regimes and rise in trade conflicts had already caused companies to contemplate weaknesses in their supply chains, whose composition principally reflected the desire to squeeze maximum value out of each stage of manufacturing. Cost minimization now requires a closer consideration of the multiple risks of disruption to the chain. Will the large-scale rollout of 5G stumble at this new hurdle? Against a backdrop of tightening budget margins for both states and companies, future technological decisions will most certainly need to balance macro and local considerations.

Via these two movements, 5G can be seen to foreshadow the international power relations that will shape the next decade. Centered around the rivalry between the US and China, they will witness the manifestation of Beijing's technological expansionism which has so far been thwarted by the Americans. Ubiquitous when it comes to connected objects and network equipment architecture, microchips are almost sufficient on their own in terms of illustrating the powerful counter-reaction which has been taking place in the US since 2019, with significant consequences for international trade. Lastly, for Europe, 5G poses the very real risk of being caught in the middle of Sino-American competition; a situation which must be very carefully navigated indeed if unduly negative consequences are to be avoided, and which could perhaps even necessitate the implementation of extraterritorial sanctions by the EU.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org