5G and the US-China tech rivalry - a test for Europe's future in the digital age: how can Europe shift back from back foot to front foot?

Rühlig, Tim; Seaman, John; Voelsen, Daniel

SWP

SWP Comment

NO. 29 JUNE 2019

5G and the US–China Tech Rivalry – a Test for Europe's Future in the Digital Age

How Can Europe Shift from Back Foot to Front Foot?

Tim Rühlig (UI), John Seaman (Ifri) and Daniel Voelsen (SWP)

Until late last year, most Europeans only knew Huawei as one of many smartphone manufacturers gaining ground in stores across the continent. But in recent months, the tech giant has turned into a symbol of a high-stakes wrestling match between the world's premier superpower, the United States, and its increasingly ambitious and capable challenger, China. Indeed, the impending rollout of 5G infrastructure has become a key battleground in a broader struggle for control over the industries of the future. Europe has meanwhile been caught on its back foot and urgently needs to develop a strategy to not only guide it through the current 5G debate, but also the tech rivalries that are still to come.

With dramatically higher data transfer speeds and decreased latency, 5G carries the promise of revolutionizing all spheres of daily life: from self-driving vehicles to healthcare to the "internet of things" and the digitalization of industrial production processes and so-called smart cities. Huawei currently leads the field in 5G infrastructure and as such, for the first time in modern history, China is in a prime position to lead the world in the rollout of a potentially game-changing technology. This prospect has caused fierce pushback from Washington and jitters across Europe and much of the West.

For months, the United States has been pressuring its European allies to enact an outright ban of Huawei from the rollout of 5G infrastructure on the continent. US Secretary of State Mike Pompeo even warned that allies who deal with the company will no longer be privy to American intelligence. China, in turn, threatened retaliation against European countries inclined to give in to US demands. China's ambassador to the European Union (EU), Zhang Ming, spoke of "serious consequences" for economic and scientific cooperation, whereas China's ambassador to Poland warned of "steep costs" for Poland if it decided to ban Huawei.

Caught between the two powers, Europe's vulnerability is clearly visible: On the one hand, European countries depend on China's central position in the value chain for information and communication technology (ICT), in particular regarding hardware; on the other hand, the United States dominates software development and remains Europe's prime security guarantor.

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Complicating matters further, the Trump administration announced on May 15 that Huawei would figure on the "Entity List" of the US Department of Commerce, effectively placing sanctions on the Chinese tech giant and banning all access to US technology (from microchips to critical software). This decision constitutes a major blow to the company that has the potential to severely affect its operations. It is also a clear signal to Western allies that the United States is serious in its campaign to stop Huawei's growing influence. For its part, China has responded with its own broadly defined "unreliable entities list" of countries, companies, or persons that "seriously damage the legitimate interests" of Chinese companies.

In this situation, Europeans risk becoming mere objects in a geopolitical struggle for technological leadership that will significantly shape our future. The defense of European interests and values in this context will require Europeans to develop a common political strategy — based on sound principles and objective criteria — for navigating the geopolitical conflicts that new technology will bring. The 5G debate adds a sense of urgency to this quest.

5G – the First "Battleground" of an Emerging Geopolitical Tech Competition

Although mobile telecommunication has always been the subject of economic competition from companies around the globe, the United States and China have a somewhat different perspective of the new, fifth generation of mobile internet. Leaders in both countries view the competition over 5G not just in commercial terms, but also as a matter of geopolitical rivalry.

The US government frames 5G as a matter of national security. This argument rests on three pillars: security, economy, and systemic confrontation.

In terms of security, the fear is that Huawei infrastructure equipment could facilitate political and/or industrial espionage. Indeed, the case leveled against the Chinese tech giant by the US Department of Justice makes it clear that American officials believe that Huawei's success is due in part to a corporate policy of espionage and IP theft. Even more importantly, intelligence agencies warn that the Chinese state could draw on Huawei to intentionally disrupt Western communication networks, particularly in the event of a major conflagration. With the connected economies of the future being highly dependent on these networks, this would likely be a tool of last resort, but one with a highly disruptive impact on the targeted society.

Economically, a core American concern is the desire to protect US industries from "unfair competition" and to avoid overdependence on the Chinese economy and Chinese technology, in particular. Central to this line of argument is the notion that succeeding in China to the degree that Huawei has no doubt requires a great deal of political connection and leverage.

Huawei is a company of strategic importance to China that receives preferential treatment, including financial, political, and diplomatic support. As with all other Chinese companies, the Communist Party is formally represented within the company with more than 300 party cells, though its actual influence is hard to gauge from the outside. This preferential treatment has the potential to threaten other vendors in a market that is already highly concentrated. Most crucially, the radio access network technology, which is essential for the rollout of 5G, is currently supplied by only three vendors at the global level, namely Huawei, Ericsson, and Nokia.

Finally, the United States perceives the rivalry over 5G infrastructure as part of a systemic confrontation. In this view, the liberal democratic world must defend itself against the increasing influence of authoritarian China. China's National Intelligence Law of 2017 (amended in 2018) requiring the country's information technology (IT) firms to "support, assist in and cooperate in national intelligence work" and the state's continuous disrespect for fundamental

principles of the rule of law are often cited in this context. On this account, Huawei is seen as part of China's authoritarian ambitions: Although a "smoking gun" has yet to emerge, the company has long been suspected of having close links to the Chinese intelligence community and the Chinese military. Furthermore, Huawei is deeply involved in establishing comprehensive domestic surveillance in China, cooperating with the Ministry of State Security by means of new, innovative technology.

However, it is not only the United States that perceives 5G through a geopolitical lens. China, for its part, aims to achieve an increasing amount of control over a broad range of economic flows through the development of infrastructure on the Eurasian landmass and beyond. Most important in this context is the country's Belt and Road Initiative (BRI), which is an infrastructure development and investment tool that has turned into China's predominant foreign policy platform. China tries to spread its influence to BRI countries by means of financing, designing, constructing, and sometimes even owning and operating digital and physical infrastructure. This helps it to gain control over flows of goods, services, and — most importantly in the context of the discussion at hand — data. Even though China does not publicly declare the geopolitical underpinnings of this initiative, Chinese strategists are aware of — and explicit about — them when speaking off the record.

In light of these geopolitical considerations on the part of the United States and China, we can expect 5G to be only the first chapter in an increasingly heated technological competition between the two political rivals, both of whom are aiming to establish, defend, or expand their geographical and sectoral spheres of influence by controlling data flows through innovative high technology.

This geopolitical take on technology is by no means without an alternative. In fact, interconnectedness has long been perceived as a global public good serving as the engine of globalization. Accordingly, does Europe necessarily need to adopt this geopolitical approach to digital infrastructure in order to succeed? Regardless of the response to this question, the EU has to respond to the geopolitical narrative and the explicit pressures placed on it by the United States and China.

Europe's Varied Responses

In late 2018, the geopolitical confrontation between the United States and China over Huawei's role in the deployment of 5G networks reached Europe. The media picked up on the reports about potential dangers emanating from Huawei's products and the growing confrontation between the United States and China, leading to questions about European governments' approaches to the issue.

Initially, it seemed that there would be a sharp split in Europe over this question. The Polish government openly called for the exclusion of Huawei after arresting and charging one of the company's employees with espionage in January 2019. The British government also seemed to be heading in that direction. At the time, countries such as Germany, France, and Italy, on the contrary, saw no reason at all to revise their policies, or at least remained largely silent on the issue. In the case of Portugal, the country's main telecoms operator even signed a contract with Huawei on 5G cooperation, just as the question was going viral. By now, however, many EU member states tend toward some middle ground: They do not want to single out Huawei but aim to formulate more general requirements for the security of mobile networks. The European Commission, moreover, has initiated an effort to coordinate member states' policies on the issue, and national governments have been asked to undertake an assessment of the risks related to 5G by the end of June.

To understand the current state of the debate in Europe, it is helpful to analytically distinguish two ways of approaching the issue: The first is openly political and focuses

on the larger geopolitical context; the second approach is primarily technical and focuses on matters of network security. The two approaches are not mutually exclusive, but in many cases, it is possible to identify what approach primarily guides a state's actions.

Approach 1: National Security and Geopolitics

The first approach situates the issue of 5G within the broader context of geopolitics. It starts from the observation that with 5G, modern societies become vulnerable in new ways. Crucially, however, it conceives of these new vulnerabilities not just as more instances of IT (in)security but as serious threats to the national security of states. In essence, this approach adopts the US perspective — perceiving 5G as one element of a multidimensional and long-term confrontation between China and the West. This conflict has a security dimension but also plays out in the economic sphere. Quite fundamentally, it is increasingly being interpreted as a confrontation between two different political and economic systems (not unlike the earlier Cold War confrontation between the United States and the Soviet Union).

This perspective also informs the risk assessment regarding the specifics of 5G: Even though there has not yet been any proof that the Chinese government has used Huawei technology to harm Western societies, the mere possibility that this might happen at some point in the future is considered reason enough to take drastic measures. Also, this perspective leads to sharp distinctions between vendors based on their political backgrounds: A company under the control of the Chinese government (directly or indirectly) is seen as a greater threat than a company from the United States, Europe, or South Korea. The goal, then, is to avoid a situation in which an authoritarian state such as China has any relevant control over critical Western infrastructure.

As described in the previous section, this approach is being pushed vehemently by the current US administration. The Australian government also has committed itself to this approach and was, in fact, the first to explicitly raise the alarm on 5G. Within Europe, states such as Poland and the Czech Republic also seem susceptible — at least to some degree — to such a perspective. In particular, the intelligence services of many states seem to share the US—Australian assessment of the threat posed by Huawei.

Since it seems almost impossible for liberal states to single out one company or country, we now observe attempts to turn this approach into non-arbitrary general principles. The main hook here is a strong emphasis on the political backgrounds of vendors. For instance, in March the German government published a (not legally binding) list of key security requirements for future networks, which starts out with the requirement that "[s]ystems may only be sourced from trustworthy suppliers whose compliance with national security regulations and provisions for the secrecy of telecommunications and for data protection is assured."

In some cases, this more openly political evaluation of vendors is furthermore combined with broad discretion for the executive. The model for this is the Australian law that authorizes the government to ban vendors "likely to be subject to extrajudicial directions from a foreign government." A new law under consideration in France, currently being reviewed by the Senate, likewise assigns the prime minister's office the responsibility to assess whether a particular vendor poses a threat to national security, without explicitly assigning responsibility to a specific agency. Although the French government would likely rely on the technical expertise of relevant state agencies (e.g., the National Cybersecurity Agency of France, ANSSI), the leeway granted to the political authorities contrasts starkly with the way the British and German governments have so far approached the issue, explicitly delegating the evaluation of these products to specialized technical agencies. Only recently did Italy adopt an approach similar to the one being debated in France.

Interestingly, the recently published "Prague Proposals" also seem mostly inspired by the geopolitical approach. These proposals were published by the Czech government after a two-day conference of 32 states from the "Western" world at the beginning of May. Although they do not represent any official consensus of the participating states, they shed light on the state of the debate. The proposals emphasize national self-determination and national security; they also include demanding political conditions that, without mentioning Huawei, seem quite clearly directed toward China: "The overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its model of governance, the absence of cooperation agreements on security". It does not come as a great surprise that the US administration publicly endorsed the Prague Proposals, whereas the Chinese Ministry of Foreign Affairs criticized them as politicizing a technical question.

Approach 2: Network Security

In comparison to a more political "national security" approach, the network security approach focuses on the security challenges of digital communication networks themselves. It thus identifies the two potential dangers of espionage and sabotage as the main challenges and aims to finding technical solutions to limit or mitigate these risks.

Even before the current 5G discussion, the United Kingdom pursued this approach by subjecting Huawei products to intensive auditing by technical specialists. The idea to exclude Huawei from the core networks but allow network operators to use the company's products for the radio access network is also guided by this approach (though, unlike with earlier mobile standards, many experts question the possibility of maintaining this distinction with 5G).

The already mentioned public statement by the German government also includes the requirement for more extensive auditing and certification of network technology. In a quite detailed manner, it also lists additional security measures such as data traffic control and transparent software deployment. Moreover, it emphasizes the need for redundancy in mobile networks and formulates the aim to avoid "monocultures" by "using network and system components from different manufacturers." Such diversity of network infrastructures, while costly, would limit the impact of an attack on any specific product.

Promoting end-to-end encryption on the application level would very likely be an effective means to protect against espionage through access on the infrastructure level. Yet, strong encryption is not high on the agenda for either the United Kingdom or Germany. Most likely, this is because the issue of encryption is controversial within these and other states: Law enforcement agencies are wary that better encryption will make their work more difficult. The problem, however, is that states thus deprive themselves of one of the most effective means to prevent espionage.

Hard Choices Ahead

The analytical distinction between the two approaches is not meant to suggest that states strictly follow one or the other. Indeed, as the example of Germany shows, many states try to combine both. Still, the two approaches inform policy-making in different ways: The geopolitical approach leads to an emphasis on openly political measures; the "network security" approach, on the contrary, focuses more on technical solutions.

When a state approaches the issue of 5G within a geopolitical framework, it would be highly questionable — if not irresponsible — not to also include many of the technical solutions proposed to increase network security. After all, if network security is seen as important enough to enter into serious inter-state confrontations, states should also do everything in their power to increase security through technical measures.

In this context, it is quite remarkable that — at least in the short term — the recent decisions by the US administration may actually create new security risks. A number of rural telecommunication operators in the United States that rely on Huawei products will not be able to receive any software updates after the 90-day "grace period," including security patches. Moreover, whereas Huawei never gained ground in the US consumer market, it is not clear what will happen to millions of Huawei mobile phone customers in Europe. They will likely not be able to update their phones with the newest versions of Alphabet's Android mobile operating system. Indeed, most likely they will have to choose between using an outdated operating system or installing an Android variant (or "fork") that builds on Android's open source components but is combined with specifications and additions provided by Huawei.

On the other hand, it is possible to focus on network security without framing the issue as one of geopolitics. States can invest to create redundant and diverse network structures and increase the auditing and certification of the technology used by network operators — all without explicitly taking sides in the geopolitical struggle between the United States and China. Right now, it seems that the United Kingdom is trying to stick to this strategy. But this approach is also political on a higher level: It avoids geopolitics at the risk of creating vulnerabilities in interactions with states that very strategically pursue their own geopolitical interests.

Most crucial in this context is that China is massively financing, designing, and constructing as well as gaining ownership and operating critical infrastructure on the Eurasian landmass and beyond, namely through the BRI. In particular, the BRI explicitly comprises a digital component, the "Digital Silk Road." The rationale behind this initiative is not just to promote Chinese high technology, but also to gain control over the flows of goods, services, and — most importantly — data. If one takes this Chinese ambition seriously, a short-term focus on network security might be seen as failing to address this more long-term strategic conflict.

In addition, not choosing a side in a context of increasing polarization could in itself be perceived as choosing China's side. The attempt to avoid geopolitics thus bears the risk of creating a serious rift with one of Europe's closest allies.

It is not surprising, then, that many states in Europe appear to be attracted to a form of "geopolitics light," combining an emphasis on network security with some more openly political measures (e.g., France, Germany). Indeed, this strategy is currently the most promising for Europe because it facilitates a degree of political and diplomatic maneuverability, allowing states the flexibility to address the perceived geopolitical risks without fully getting drawn into the confrontation between the United States and China.

The challenge with this strategy, however, is that "geopolitics light" is still geopolitics. When states in Europe decide to deny, or seriously restrict, market access for companies from specific countries — be it China or other states — these states will perceive such restrictions as geopolitically motivated. Thus, when considering "political" criteria in the context of the debate on the security of 5G networks, states must be clear about what level of geopolitical confrontation they deem necessary to defend their security interests — and what level of confrontation they are willing and able to endure. The trick is identifying what dose of politically and strategically motivated considerations would be sufficient without unnecessarily widening geopolitical rifts that paint all future tech competition in a clearly confrontational light.

The distinctly geopolitical goal here would be to not only increase network security but to also defend the principles that are constitutive of Europe's political order. These include an emphasis on the rule of law, democratic accountability, as well as a commitment to fair competition. The question, then, is what measures would be

necessary to defend these principles? Requirements for more transparency of vendors — both in terms of their financial workings as well as concerning their corporate governance structures — for instance, could be a necessary means to protect the European model of rule of law. The challenge, however, is to use such requirements in ways that do not themselves undermine basic principles of the rule of law; that is, it must be ensured that such requirements are applied in a non-arbitrary way that provides those affected with effective means of contestation.

Pressing Questions

All over Europe, the deployment of 5G networks will soon begin. In the coming months, Europeans will have to settle on what their approach to the issue will be. The recent decisions by the US administration have made this even more difficult. If the United States upholds its export restrictions, this may seriously impact Huawei's ability to offer its products and services. In fact, to the extent that Huawei depends on US companies to provide hardware components for their network technology (e.g., semiconductors), the company may simply not be able to offer its products and services to European telecommunication companies. The US export restrictions would thus effectively render the European debate on Huawei as merely being theoretical.

In this particular situation, thus, Europe has become a bystander, at least for the moment. If Europe wants to defend its own interests — not only in this particular case, but also with regard to the larger tech rivalry between the United States and China — its member states will have to be very clear about their interests as well as the adequate means to pursue them. To this end, we want to emphasize four questions that seem most pressing to us.

(1) What is the cost of security? From a technical perspective, promoting the diversity and redundancy of network infrastructure is the best way to protect against network disruptions. Yet, this extra level of security is costly, like any backup system. So if states are serious about the need to protect digital infrastructure, they will also have to engage in an open debate about these costs. Moreover, they will have to develop new governance mechanisms for ensuring that the private companies which operate the networks fulfill these criteria. After all, this requires a detailed level of centralized planning to coordinate the activities of all the network operators involved.

(2) How can "political trustworthiness" be objectively assessed? The idea of political "trustworthiness" is inevitably vague. If states want to take into account the political backgrounds of companies involved in providing critical public infrastructure, they will need to define more specifically what kind of political commitment they expect from these companies. What is uncontroversial is that companies operating in a state must abide by that state's laws. The more specific fear, however, seems to be that some companies are unduly influenced by their home state's governments. In some cases, that may well be the case. The questions, however, are what counts as sufficient proof of such undue influence, and, on the other hand, what serves to render a company as "trustworthy"? If European states cannot offer clear and objective criteria for the requirement of "trustworthiness," any decision on these grounds will be perceived as arbitrary — and thereby threaten the European legal order.

Even more fundamentally, the issue of trustworthiness seems to go beyond individual companies. Despite all the focus on Huawei, the real issue seems to be whether the Chinese state can be sufficiently trusted not to use Chinese companies to harm European states. In addition to measures aimed at companies, another option could thus be to explicitly address these issues in diplomatic relations with China.

(3) Can Europe find consensus and forge its own path? In their dealings with the issue, the states in Europe should also consider the impact of their actions on the

European Union as a whole. A joint and coordinated EU approach promises not only a higher level of security but also seems necessary to formulate an independent position in the geopolitical confrontation between the United States and China: Only a united Europe will be able to forge its own path in terms of digital technology and protect itself against possible Chinese or American retaliation. In a first positive sign, the heads of states and governments of all EU member states launched a process of coordination on March 22 at the meeting of the European Council. Here, Europe can and should build on its success in drafting new data protection regulations and in establishing an EU-wide screening mechanism on foreign investment.

The ongoing process of coordination launched in March by the European Council finds its legal basis in two cybersecurity documents (i.e., the Directive on Security of Network and Information Systems of 2016 and the new EU Cybersecurity Act, which was adopted by the European Parliament in March 2019) as well as in the EU's telecommunication rules, which entered into force as early as 2009.

Other fields to consider a common approach include competition law and public procurement rules, which could help prevent over-dependencies from individual companies and — potentially, if European law is revised accordingly — from groups of companies from one country.

Finally, the China strategy of the EU and in some of its member states (e.g., the Netherlands) is undergoing a fundamental shift. The EU seems to agree more and more that China should be considered a partner, a competitor, and a strategic rival at the same time, depending on the specific context and the policy field. Technological competition and Europe's dependence on global ICT supply chains should be included more systematically in this context and become an integral part of the EU's Common Foreign and Security Policy. Hence, we consider it a positive and logical step that the issue is currently being discussed not only in institutions dealing with network security (such as DG Connect and the European Union Agency for Network and Information Security, ENISA) but also within the European External Action Service, which is coordinating a member states-driven process as part of the Union's foreign policy.

(4) What lessons can we draw from other partners on hedging geopolitical risks? While Europe is still grappling with finding its own approach, it should also closely monitor what is happening in other regions of the world. For both China and the United States, Europe is only one part of their geopolitical contest. Indeed, some variation of the European 5G debate can be observed in many states, from technologically advanced economies such as Japan and South Korea to developing countries throughout Africa and Southeast Asia. Europe might do well to engage with these countries in an exchange on how to deal with the threat of becoming a mere object in geopolitical power games.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1861-1761
doi: 10.18449/2019C29

Dr Tim Nicholas Rühlig is a Research Fellow with the Europe and Asia Programs of The Swedish Institute of International Affairs (UI). John Seaman is a Research Fellow in the Center for Asian Studies at the French Institute of International Relations (Ifri). Dr Daniel Jacob is an Associate in the Global Issues Division at SWP.