INSTITUT
MONTAIGNE

Europe and 5G: the Huawei Case

NOTE JUNE 2019

INSTITUT
MONTAIGNE

Europe and 5G: the Huawei Case

NOTE - JUNE 2019

There is no desire more natural
than the desire for knowledge

SUMMARY

INTRODUCTION

Huawei has won many 4G markets and achieved a breakthrough in world market share for smartphones. Its seemingly omnipresent 5G offering now sparks controversy and also sheds light on strategic issues which were conspicuously absent from previous mobile network generations. There are good reasons for this, which are linked both to the nature of 5G and to specific features of the Huawei company.

Let's start with 5G. As is well-known[1], it is not simply about increasing by 2025 the speed of communication between individuals, even if mobile phones will also enjoy higher speed and shorter latency time. The consequence of 5G high speed and larger flow is a multiplicity of new uses, which are as impossible to anticipate as web applications were in their time. Digital factories, particularly the multiplication of 3D production, telediagnosis and remote surgery, extensive new networks and the spread of the Internet of Things, starting with self-driving vehicles which are its most advertised feature, the supremacy of digital clouds over localized servers, artificial intelligence and modernized public services are only a few of the foreseeable consequences. Whoever will extract or own big data and algorithms in real time will dominate industry, services and also a number of confidential aspects of human life. The reliability and security of data flows, the risks of theft, hacking or sabotage will be much more important than in the previous internet generation.

5G must therefore be considered as a critical infrastructure. It will impact all economic activities, with consequences both positive and negative. It will very quickly spark a generational leap for the companies and services which adopt digital manufacturing, and therefore disadvantage companies or regions which remain outside its deployment. Just as 4G favored the emergence of the web giants, 5G will be the springboard for emerging major players. Conversely, extended digitalization raises data protection problems on an unprecedented scale. It is easy to imagine risks of sabotage for distribution networks and public services, such as the remote takeover of autonomous cars, medical apparatus or the shutdown of entire factories. 5G is both a promise of unprecedented productivity, a risk of stalling competitiveness for whole swaths of the European economies, and also a question of national security and sovereignty.

The choice of operators, infrastructures and their suppliers is more than simply a question of business and cost opportunity. Data confidentiality and the security of data

[1] "5G in Europe, Time to Change Gear!", Policy Paper, Institut Montaigne (May 2019), https://www.institutmontaigne.org/en/publications/5g-europe-time-change-gear-part-1

flows, including from foreign interference, represent a major challenge. In this area, Europe has much ground to cover in order to catch up. Europe, which once created the GSM standard, today finds itself fragmented into national markets, each of them structured by three to four operators and a bevy of mobile virtual network operators (MVNOs). The short-term benefits from open competition for consumers come at the price of low investment capacities for operators and manufacturers and, as will soon become clear, insufficient control over the 5G standard itself.

This is where Huawei comes in. The Chinese – and now global – telecommunication giant operates in a class of its own.

I

HUAWEI, SPEARHEAD OF CHINESE TECHNO-NATIONALISM

The company was created in 1987 in South China with a capital of 21000 yuan by a Chinese army veteran engineer trained in cryptography and electronic transmission. The group's former number 2, Sun Yafang, is said to have worked in the Communications Division of the Ministry of State Security. Such links to the security apparatus can be found elsewhere, in many information technology companies and for example in many of Israel's digital start-ups. New research has also underlined the peculiar ownership structure of Huawei, a company which claims that its employees are its sole owners.[2] Although he today holds only 1.14% of Huawei's capital, Ren Zhengfei seems, with his family, to exercise complete control over the company, which is in the hands of an entity sometimes called an employee union. More accurately, this is a virtual scheme of share ownership, renewed every year and giving employees very restricted and profit-linked rights for the duration of their contract in the company. In the 1990s, Huawei was perhaps one of those many cases of hybrid companies halfway between state companies and much-smaller true private enterprises. The actual composition of this virtual shareholding is unknown, although Huawei now claims it is available for consultation by anyone. In practice, in the digital age, it is said to take the form of large paper registers kept in a glass tower! The ownership structure (Huawei Trade Union Committee owns 99% of Huawei Holding which in turn owns Huawei Technologies) suggests indirect control by the Party, since all trade unions in China are subject to Party authority. These ambiguities surrounding Huawei ownership are a throwback to the structure of the Chinese economy at the time of the company's founding. In the second half of the 1980s and at the start of the 1990s, there were many new companies in China of the third type, in Chinese "mixed ownership" (混合所有制), which combined different forms of ownership.

The murkiness of the actual ownership arrangements is compounded by that of the financing sources that have enabled the rise of Huawei. Before 2011, more than 30 billion dollars in loans on preferential terms were granted to Huawei (and also to its competitor ZTE) in China.[3] They came mostly from the China Development Bank (CDB),

[2] Christopher Balding and Donald C. Clarke, "Who Owns Huawei?" SSRN *Electronic Journal* (2019) http://dx.doi.org/10.2139/ssrn.3372669. Filip Jirouš and Jichang Lulu, "Huawei in CEE: From 'Strategic Partner' to Potential Threat," E-International Relations (2019), https://sinopsis.cz/en/huawei-in-cee-from-strategic-partner-to-potential-threat/ Bob Seely, Peter Varnish Obe, John Hemmings, "Defending our Data, Huawei, 5G and the Five Eyes", Henry Jackson Society (May 2019). https://henryjacksonsociety.org/wp-content/uploads/2019/05/HJS-Huawei-Report-A1.pdf

[3] Matthew Dalton, "EU Finds China Gives Aid to Huawei, ZTE," *The Wall Street Journal* (2011), https://www.wsj.com/articles/SB10001424052748703960804576120012288591074

the foremost "policy bank" of the Chinese party state, which openly acknowledges a close relationship with Huawei. Over the 2012-2018 period, total financing from CDB and Eximbank for overseas projects has reached 9.8 billion dollars.[4] It also appears that a national preference may have been established in China. On this basis, Huawei dominates the market for Chinese 4G mobile network gear. This is in spite of the fact that its prices on the Chinese market can be 25% higher than those of a European competitor like Ericsson, as shown by a recent tender.[5] In the context of an upcoming 5G rollout, the issue of subsidies in China raises the familiar issue of reciprocity with Europe.

Huawei's links with the army and cyberespionage are another shadowy area. On the eve of the fall of the Afghan Taliban regime, Huawei signed a contract to supply an optical fiber network to the latter - as it was to do with Iran. These are deals which could hardly have been inked without the support of the People's Liberation Army.

Overall, the link with the Chinese party-state is indelible owing to the nature of the political system in China. It is reflected in the penetration of Huawei by the Communist Party - an unavoidable feature in China. Regarding the 300 cells and 12,000 members of the Party among Huawei's 160,000 employees, the company's Party secretary Zhou Daiqi underlines that this arrangement is in "compliance with Chinese law, that the function of the cells is to help to improve the quality of life of the employees and ensure that they respect the company's ethical principles, but the cells do not interfere in management and political choices."[6] Indeed, the power of the Party over companies need not be asserted in everyday business - it may only reveal itself at decisive moments.

China deploys an impressive array of support for Huawei. It is no surprise that several levels of the Chinese state are directly involved in defending Huawei against the attacks on the company. Minister of foreign affairs Wang Yi recently emphasized that Huawei should under no circumstances behave like a "silent lamb," that China reserved the right to respond "by all necessary means" to the attacks against Huawei, that it was a matter of defending the "legitimate development interests of a country and its

[4] "A Transactional Risk Profile of Huawei," *RWR Advisory Group* (2018), https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf

[5] Davy Zhu, "Ericsson Is Surprisingly Cheapest Vendor in Huawei's China," *Bloomberg* (2019), https://www.bloomberg.com/news/articles/2019-02-14/in-huawei-s-china-ericsson-is-surprisingly-the-low-cost-vendor

[6] "互联网公司在招聘上不要党员？" (Do Internet companies Reject the Job Applications of Party Members?) (2016), http://www.sohu.com/a/100572816_359612

nationals."[7] The Ministry of State Security has arrested several Canadian nationals in retaliation against the extradition procedure to the United States initiated by Canadian courts against Huawei's financial director Meng Wanzhou.[8] China feigns ignorance of the fact that this was a legal obligation for Canada arising from its extradition treaty with the United States and not a political decision.

Language is not neutral and correlations can be revealing. When Wang Yi labeled Huawei a silent lamb, he could not be unaware of the term "wolf culture" (狼性文化), popularized by Ren Zhengfei himself to motivate his employees.[9] Over the years, the wolf metaphor has become a badge of identity for Huawei, reflecting a corporate culture which promotes ambition, risk-taking, and an *eat what you kill* mentality inspiring its aggressive expansion in Chinese and international markets. During the 1990s, in addition to "wolf culture," the slogans motivating the Huawei staff drew on near-military images of survival and combat. They included sentences such as "the bird that burns without dying is a phoenix" (烧不死的鸟是凤凰), "let's raise a glass when we win and defend ourselves at the price of our lives when we lose" (成则举杯相庆，败则拼死相救), together with many references to Lei Feng, the mythical model worker of the 1960's and a figure still used in Chinese propaganda for domestic use. Huawei's corporate charter, adopted in 1998, wholeheartedly endorses economic patriotism: "serving the prosperity of our great mother-country, serving the great rejuvenation of the Chinese nation" (为伟大祖国的繁荣昌盛，为中华民族的振兴).[10] Very recently again, Meng Wanzhou, Ren Zhengfei's daughter, has described the company as a "fortress" (堡垒) in a letter to Huawei's employees.[11]

While Huawei's communication in China draws upon martial phraseology and communist imagery, its approach is quite different outside China. In Europe, the chairman of the Huawei board proclaims his "confidence in openness and innovation,"

[7] Ben Blanchard, "No 'silent lambs': China Supports Huawei's Bid for U.S. legal redress," *Reuters* (2019), https://www.reuters.com/article/us-china-parliament-huawei-tech/top-chinese-diplomat-says-supports-huaweis-bid-for-legal-redress-idUSKCN1QP089

[8] Chris Buckley and Catherine Porter, "China Accuses Two Canadians of Spying, Widening a Political Rift," *The New York Times* (2019), https://www.nytimes.com/2019/03/04/world/asia/china-canada-michael-kovrig-huawei.html

[9] 杨媚, "华为总裁任正非：缔造"狼性文化"," (Huawei CEO Ren Zhengfei on Building a Wolf Culture) *中国企业报* (2011), http://dangjian.people.com.cn/GB/240027/17578570.html

[10] "《华为基本法》是什么？" (What is Huawei's Corporate Charter?) (2016), http://www.cghuawei.com/archives/2149 Full text: http://blog.sina.com.cn/s/blog_6263274c0102wg41.html

[11] "孟晚舟听证会后致信华为人：心中从未如此丰富而广阔，谢谢你们," (Meng Wanzhou's Letter to Huawei Staff After Her Hearing: My Heard Has Never Been That Rich and Wide, Thank You) (2019), https://www.guancha.cn/economy/2019_05_13_501337.shtml

and in the United States, Huawei sometimes labels itself as a "sesame seed."[12] In Europe, on social media, and in the press, Huawei is a key player whose public relations effort allows unequaled media coverage. Throughout the continent, criss-crossed by Huawei's 5G roadshow bus, the company is running a talent recruitment program called *"seeds for the future."*[13] The company is recruiting in security and defense circles, with choice catches such as Andrew Hopkins, ex-deputy director of GCHQ, the UK electronic intelligence service.[14] The Polish Orange employee accused in January 2019 of spying in connection with a Huawei manager was a former Polish counter-intelligence officer. Huawei does not supply information on its website about the composition of its International Advisory Council, whereas some press articles mention its existence. In 2013, according to sources in the EU's DG Trade, Huawei was the multinational firm which spent the most on lobbying in Brussels. In 2017, according to its compulsory declarations, Huawei spent 2.19 million euros on lobbying in Brussels.[15] It also sponsored many public events throughout Europe according to its website.[16]

These native links with the backbone of the Chinese political system point to the importance of Huawei's immense success in the light of Xi Jinping's national project, as outlined with great clarity in a roadmap presented at the 19th Communist Party Congress in November 2017: China's transformation into a "global innovation leader" by 2035, then a "global leader in terms of composite national strength and international influence" by 2050.[17]

[12] Yang Ge, "Huawei Is 'Sesame Seed' Under Attack from U.S. 'National Machine,' Chairman Says," Caixin (2019), https://www.caixinglobal.com/2019-02-18/huawei-is-sesame-seed-under-attack-from-us-national-machine-chairman-says-101380966.html

[13] Huawei, Huawei 5G Truck Bring 5G to Public and Invite Ecosystem to Explore 5G Together (2018), https://www.huawei.com/en/press-events/news/2018/11/Huawei-5G-Truck-Public-Invite-Ecosystem

[14] Tamlin Magee, "Huawei Controversies Timeline," *ComputerWorldUK* (2019), https://www.computerworlduk.com/security/huawei-controversies-timeline-3692840/

[15] "Huawei Technologies (Huawei)," LobbyFacts (2019), https://lobbyfacts.eu/representative/c6677e9de90e4a2c86e5640c83e3dfbc

[16] "Events," *Huawei* (2019), https://www.huawei.com/en/press-events/events

[17] "Full text of Xi Jinping's report at 19th CPC National Congress," Xinhua (2017), http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.htm

II

HUAWEI AND THE SECURITY OF EUROPE, A MISTAKEN DEBATE

Huawei is at the heart of Europe. Out of the 105 billion dollars of income earned by the company in 2018, 24.3% came from the Europe/Middle East/Africa region and 40.8% from the equipment contracts with telephone operators.[18] Huawei holds 17.5% of the smartphone market in Europe, behind Samsung and Apple.[19]

Does the company constitute a risk for the national security of European states? If Huawei has always failed to demonstrate the opposite, its critics have sometimes provided pointers to likely Huawei involvement in cyberespionage operations, but not decisive evidence. Let's cite the main cases: that of the African Union, the international organization based in Addis-Ababa, is indisputably the most striking. Since 2012, Huawei had been the almost exclusive supplier of integrated IT solutions, from server to cloud wifi and local data storage. From 2012 to 2017, every night between midnight and two in the morning, all the collected data was sent to an unknown server in Shanghai… Although it is possible that random flaws in the Huawei solutions explain this leak, it is inconceivable that the company could have failed to detect them for five years. Another case concerns Huawei's links, in 2015-2016, with a Chinese company, Boyusec, convicted of cyberespionage in the US, and the links of these two companies with the Chinese cyberhacker group APT-3. In 2015 and 2016, malware was detected in several models of smartphones sold by Huawei, Lenovo and Xiaomi, giving access to some of their contents.[20]

The fifth annual report by the Huawei Cybersecurity Centre in the UK, funded by Huawei but supervised by the British security services, including GCHQ, sheds a different light.[21] It concludes that "Huawei's approach to software development raises significant risks for UK operators (…) and the oversight board is only able to provide limited assurances that the risks raised by Huawei equipment deployed to date in the UK can be managed." The software deployed by Huawei is defective and contains

[18] Huawei Investment & Holding Co., Ltd., *2018 Annual Report,* https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report2018_en_v2.pdf?la=zh

[19] "Mobile Vendor Market Share in Europe - April 2019," *StatCounter* (2019), http://gs.statcounter.com/vendor-market-share/mobile/europe

[20] Julien Lausson, "Des malwares pré-installés dans des mobiles Huawei, Xiaomi, Lenovo…" (Malware installed in Huawei, Xiaomi and Lenovo phones) *Numerama* (2015), https://www.numerama.com/magazine/34130-malwares-mobiles-chinois.html

[21] "Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2019," *Gov.UK* (2019), https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

many flaws ("several hundreds of vulnerabilities"), which have not been mitigated by Huawei. The context, particularly the apparent use of an out-of-date OS purchased from a third party company, also suggests that the poor quality of the Huawei software is not necessarily intentional: it could originate quite simply in a greater indifference to security in the context of the Chinese economy and in a race for immediate effectiveness. Some recent affairs instill additional doubt regarding the existence of vulnerabilities installed on purpose: with Vodafone, in Italy, and in the Netherlands.[22]

Huawei admitted this weakness in its last annual activity report.[23] The report emphasizes an investment of 2 billion dollars approved for the improvement of Huawei's software engineering capability in 2019. For the company, this is a necessary qualitative step at the time of the transition to 5G, since the operation of the networks will rely heavily on its software infrastructure. The British report refused to acknowledge this new effort, as Huawei did not provide any details about the investment. There was also confusion, as Huawei communicated about an investment of 2 billion dollars (or 23% of its net global profits in 2018) only for the securing of its gear in the UK, whereas its annual report appears to state that this is an R&D investment towards its global growth.[24]

The work done by the British cybersecurity services is particularly important, as this is the European country most committed to Huawei in the past – 70 % of the country's 4G infrastructure was built by Huawei. The UK has learned from this, since British Telecom has announced the removal of the Huawei gear already installed in 4G core networks.[25] A debate is now raging in the UK on the scope to be left to Huawei in the construction of the 5G infrastructure. All telecommunications networks are vulnerable to spying, sabotage and blackmail in the event of a confrontation with a state that possesses the required capacity. Huawei's flaws, like those of any other network equipment supplier, can also be exploited by any intelligence service with sufficient technical capability. The British authorities are now applying a retrospective safety first principle to 4G core networks. Yet this does not mean that the debate on 5G is closed.

---

[22] Daniele Lepido, "Vodafone Found Hidden Backdoors in Huawei Equipment," *Bloomberg* (2019), https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment. Huib Modderkolk, "Huawei mogelijk betrokken bij Chinese spionage in Nederland," deVolkskrant (2019), https://www.volkskrant.nl/nieuws-achtergrond/huawei-mogelijk-betrokken-bij-chinese-spionage-in-nederland~b4fadc1c/?referer=https%3A%2F%2Fwww.forbes.com%2F

[23] Huawei Investment & Holding Co., Ltd., *2018 Annual Report,* https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report2018_en_v2.pdf?la=zh

[24] Jack Stubbs, "Huawei $2 billion security pledge followed walkout by British official - sources," *Reuters* (2018), https://uk.reuters.com/article/uk-huawei-europe-britain/huawei-2-billion-security-pledge-followed-walkout-by-british-official-sources-idUKKBN1OC23Q

[25] Alex Hern, "BT removing Huawei equipment from parts of 4G network," *The Guardian* (2018), https://www.theguardian.com/technology/2018/dec/05/bt-removing-huawei-equipment-from-parts-of-4g-network

The second important distinction to make is that the cases of Chinese industrial espionage documented in open source have been usually based upon entry points other than control of network gear: phishing, human errors and software vulnerability.[26] In the public domain, there exists only one case reported by the Australian intelligence services of Chinese spying by means of Huawei-supplied codes allowing intrusion into a network built by the OEM.[27] There is little documentation on this case. Everything points to Huawei gear being highly vulnerable and the company closing its eyes in some cases, but there is no public evidence to suggest that Huawei is installing back doors in its network architecture on behalf of the Chinese intelligence services. On the other hand, the history of the company features cases of espionage and intellectual property theft involving some employees in the US. If it takes place, the trial of chief financial officer Meng Wanzhou after her extradition to the US will determine to what extent Huawei has set up a fraud scheme to violate United Nations sanctions towards Iran.[28]

In a 5G ecosystem, many potential flaws can be exploited by ill-intentioned groups, especially as the balance between the sophistication of hackers and the updates of defensive systems will be perpetually changing. A "my word against yours" approach to deal with the risk of a Trojan horse conceals the fact that any supplier's gear will not be the only entry point to be secured when managing cybersecurity in a 5G architecture. The 5G ecosystem multiplies vulnerabilities at different network entry points, creating new challenges for the security of data flows which do not arise only from the architecture of the core networks and radio equipment. The software architecture of the network, data storage in the cloud, and connected objects are the most obvious vulnerability points, which will call for new defensive measures to be taken by operators – and by states.

On the other hand, there is no question that the Huawei case is also an issue of trust. The company has badly managed the controversy about its obligations towards Chinese law. Article 7 of the 2017 National Intelligence Law stipulates that all entities "and citizens shall, in accordance with the law, support, provide assistance, cooperate in national intelligence work, and guard the secrecy of any national intelligence work

[26] Jan-Peter Kleinhans, "5G vs. National Security - A European Perspective," *Think Tank für die Gesellschaft im technologischen Wandel* (2019), https://www.stiftung-nv.de/sites/default/files/5g_vs._national_security.pdf

[27] "China Used Huawei To Hack Network Says Secret Report," *The Australian* (2018) https://www.theaustralian.com.au/nation/china-used-huawei-to-hack-network-says-secret-report/news-story/510d3b17c2791cbcac18f047c64ab9d8

[28] "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud," *The United States Department of Justice* (2019), https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial

that they are aware of."[29] This article has seriously damaged Huawei's credibility. The company cannot reinvent the balance of institutional power in the Chinese system. The judicial power is subordinate to the executive and the latter to the Party. The absence of separation of powers is a defining feature of Leninist regimes, and theorized as evidence of superiority over democratic systems.

In this context, blanket denial, including from Ren Zhengfei, who broke his silence on this occasion to proclaim that even if Xi Jinping himself ordered him to use Huawei equipment for spying, he would not obey "by virtue of the Constitution", fails to be convincing.[30] Between the executive branch of Chinese power and the business world, whether public or private, the relationship is such that no economic actor can hope to turn down a demand from the party state without paying a high cost. This is eloquently demonstrated by the sudden disappearances of business leaders over the past few years, from Fosun to Anbang, CEFC and HNA.[31] In its legal argument, Huawei emphasizes the legal protection granted to businesses in Chinese law and the primacy of the privacy protection principle in the Constitution of the PRC (article 40, which limits this protection in national security cases).[32] These arguments do not stand up to observations of arbitrary rule in the exercise of power in China.

There is a certain irony in the fact that the intelligence law, resulting from an administrative initiative aiming to clarify the obligations of each actor in China, provides an argument against Huawei to officials in Europe or the US who are translating onto the Chinese system the workings of their own rule of law. The private sector's obligations towards the executive are of a political nature, well beyond any formal regulation. But the unique feature of the Xi Jinping era is the sustained effort to enshrine into law the Party's domination over many aspects of state governance. It is revealing that the formulation "the Party leads everything" (党是领导一切的), was added to the Charter of the PCC in the wake of its 2017 19th Congress.[33]

---

[29] "National Intelligence Law of the People's Republic of China (2018 Amendment) [Effective]," *Standing Committee of the National People's Congress* (2018), http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law

[30] "Huawei founder says he would defy Chinese law on intelligence gathering," *CBS News* (2019), https://www.cbsnews.com/news/huawei-president-ren-zhengfei-says-he-would-defy-chinese-law-on-intelligence-gathering/

[31] Ann M. Simmons, "Some of China's richest and most powerful men have mysteriously vanished," *Los Angeles Times* (2017), https://www.latimes.com/la-fg-china-billionaires-vanish-20170614-story.html

[32] "Is Huawei compelled by Chinese law to help with espionage?" *Financial Times*, (2019) https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0. See also: "Chapter II The Fundamental Rights and Duties of Citizens" Constitution of the People's Republic of China (2004), http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_1372964.htm

[33] 薛万博, "怎样认识"党是领导一切的"写入党章？" (How to understand the inclusion in the Party Charter of the Party leads everything?" *CPC News* (2018), http://cpc.people.com.cn/n1/2018/0125/c123889-29787340.html

The debate on Huawei's failures to secure data is a real one, even if evidence of actual complicity in an act of cyberespionage is missing: only the African Union case comes close. Countermeasures exist, but their effectiveness is limited when confronted with this reality: Huawei and its executives could under no circumstances oppose a penetration or sabotage action by the intelligence services of their country, even if they knew about it. It is then up to each party to evaluate the scope of a necessary precautionary principle, including with respect to suppliers of other nationalities, along with the special risk which may result from the actions of these intelligence services and their accomplices – organized hackers and close allies such as North Korea. This risk will be ever-changing. It is also obvious that there are European countries, not to mention the operators themselves, which, even if they are aware of these risks, do not have the technical and human resources to ward off these.

III

A FRAGMENTED EUROPE

While the commercial rollout of 5G has started in the US and South Korea, Europe has progressed unevenly. There is a dual fragmentation of Europe: it concerns the broadband spectrum auctions and security standards. Each rollout is on a national basis, with a multiplicity of operators investing large sums to obtain a share of the broadband spectrum from each member state. This leads to a market led by cut-throat price competition. The commendable efforts of the European Union have focused above all on visibly serving consumers - particularly cutting the cost of voice calls and data flows within the EU. While laudable, this policy also reduces ARPU (Average Revenue Per User) and hence the available margin for investment of European operators into the network infrastructure of the future China, endowed with a market on an immense scale, a tiny number of operators, and massive subsidies for the introduction of new standards, has very similar revenues per user. In the US, the concentration of operators, criticized in terms of insufficient competition, yields much more comfortable revenues.

This market structure explains why European countries are at differing stages in the construction of their 5G infrastructure. In the absence of a single telecom market within the EU, each country is responsible for organizing an auction for the assignment of 5G rollout frequencies. This is a political step - the auction rules set domestic coverage and service quality requirements, determine the rollout schedule and settle the number of network operators. This fragmentation has contributed to Europe, which once generated the GSM standard, losing the leadership in the creation of 5G standards. Huawei is today in the lead for the number of 5G patents, ahead of Nokia, LG, and Ericsson.[34] From Huawei's standpoint, the advent of 5G represents a qualitative leap since the company is among the leaders in defining codes and standards, particularly within 3GPP, a consortium of organizations for the development of telecommunications standards, which is working on harmonizing them.[35] From the point of view of European interests, this change underlines that Europe has started to fall behind.

The long-term consequences are clear. China has an investment plan for the coming three years evaluated at between 180 and 220 billion dollars - an amount which is

[34] Shuli Ren, "China's 5G Riches Are a Blocked Number for Investors," *Bloomberg Opinion* (2019), https://www.bloomberg.com/opinion/articles/2019-02-11/china-s-5g-winners-are-out-of-reach-for-stock-investors

[35] "About 3GPP Home," 3GPP, https://www.3gpp.org/about-3gpp/about-3gpp

not even unduly high when compared to the 800 million mobiles and the billions of connected objects to come. Europe is short of investments and lacks collective planning of the 5G infrastructures: to our knowledge, only five Nordic countries (Finland, Sweden, Denmark, Norway and Iceland) have a collective network project.[36] At this stage, many sources underline that, as with 4G, Huawei is indeed the supplier with the lowest costs and the most extensive backward compatibility with earlier standards (together with Nokia for this last point). The company has also been clever enough to promise many research centers and university link-ups throughout Europe, a money-spreading exercize which is also a tool for recruiting qualified labor. Whether the focus is on ultimate security or industrial independence, the precautionary principle has been a secondary or non-existent consideration for most states and operators.

Our interactive map showing Huawei 5G rollout and penetration in Europe reveals this fragmentation[37]. The map gives access to detailed sheets for thirty European countries (the 28 EU members, Norway and Switzerland), which contain data on the 5G rollout status and Huawei's presence in the telecom infrastructure in each of the countries, based on criteria listed in a methodological note. Huawei has already signed partnerships with 14 European operators for the construction of the 5G infrastructure. The company has announced 23 sales contracts in Europe, which include partnerships with operators even if not all the contracts are effective yet.[38] Now in many countries, auctions to assign the 5G frequencies had not yet been launched by the spring of 2019. Huawei has a significant presence in 5G pilot projects throughout Europe, most often on a city scale and sometimes in central districts such as Mitte in Berlin and Westminster in London. In several countries, a strong Huawei presence is seen in 4G radio networks, in contracts with operators for the construction of a cloud infrastructure, and in fiber optic communications. Huawei also invests in security centers in the UK, Germany, and Brussels and has launched many partnerships in education, training and research, via university tie-ups or special-purpose programs.

There also exists a more difficult-to-quantify dimension of Huawei's presence in Europe: the nature of the public debate on the company's presence. In some

[36] "5 Nordic Countries aim to be 1st interconnected 5G region in the world," *IEEE Communications Society Technology* Blog (2018), https://techblog.comsoc.org/2018/06/06/5-nordic-countries-agree-to-accelerate-5g/

[37] Link to the interactive map : https://www.institutmontaigne.org/publications/leurope-et-la-5g-le-cas-huawei-partie-2#section4662

[38] "Huawei reveals it has no 5G contracts from mainland China," *Financial Times* (2019) https://www.ft.com/content/c6f8da24-6023-11e9-a27a-fdd51850994c?shareType=nongift

countries, the political class has grasped the security risk issue, whereas in others, Huawei's activities are not at all seen in that light. Thus, whereas Valletta, Monaco, and Duisburg have begun the construction of smart cities with Huawei and a large part of the Italian political class is giving the Chinese manufacturer its strong support, the discussion in other countries has moved towards greater security emphasis. In these debates, Huawei is anything but passive, even if its public relations campaign differs in intensity from country to country.

These criteria enable an overview of Huawei's diversified presence in Europe, at a time when crucial 5G choices are being made. Taking all factors into account, Italy, Poland, Spain, Latvia, the Netherlands, Portugal, and Malta exhibit the strongest presence of Huawei. At the other end of the spectrum, Slovenia, Estonia, Denmark, and Norway are difficult hunting grounds for Huawei, while Croatia and Cyprus have fallen behind in the construction of their telecoms networks.

The decisions to be made for 5G cannot be reduced to a rational choice based on quality/price trade-offs for consumers. Under these circumstances, the fragmentation and near-cacophony in Europe with respect to the Huawei case make it much more difficult to apply a coherent, continent-wide approach. This approach should take into account not only the security risks but also geopolitical challenges and issues of relative power, towards which technological and economic primacy are of course key factors. The precautionary principle is far from being applied everywhere. The European states diverge in their security codes and standards for telecom gear - this is the second major area in which Europe is fragmented.

The European Commission has taken up this critical issue of the convergence of standards in Europe. Its March 2019 recommendation describes 5G security as a "strategic autonomy" issue for the EU.[39] It is pushing for convergence of risk assessment and security practices between countries, imposing a timetable on those which did not have one for the conduct of a national review of 5G-related vulnerabilities (results to be submitted on July 15, 2019 to the Commission and to the European Cybersecurity Agency). It highlights the EU instruments for contributing to 5G regulation in Europe: the General Data Protection Regulation, which sets out obligations for the use of personal data, and the new framework for the screening of foreign investments which creates provisions for infrastructure protection within the Union. The statement emphasizes the central role of the

[39] "European Commission recommends common EU approach to the security of 5G networks" *European Commission – Press Release* (2019), http://europa.eu/rapid/press-release_IP-19-1832_en.htm

European Cybersecurity Agency (ENISA) and its introduction of a continent-wide equipment certification system benefiting from national practices which are diverse and undergoing reform in many member states. It extends the initiative begun by the 2018 European Cybersecurity Act,[40] which already created an EU certification framework for cybersecurity.

As in other sensitive areas such as foreign investment or export controls, the EU is now compelled to harmonize wide-ranging practices, compile information coming from the member states and identify and promote best practices. The Commission has set a December 31, 2019 deadline for drawing up a list of security risks and possible mitigating measures.

On May 15, 2019, Donald Trump announced the exclusion of Huawei from authorized suppliers in the United States, citing the International Emergency Economic Powers Act. This decision was immediately followed by the Department of Commerce's placement of the company on the "entity list," a list of entities or individuals with which US companies cannot trade without a special authorization that in practice is almost impossible to obtain. This is a game changer. Far beyond the security of networks, it targets all three of Huawei's main business segments: network equipment, smartphones, and business-to-business services. The US decision presents Huawei's foreign partners with a dilemma: follow the US decision, or on the contrary, seize business opportunities arising from the ties that are severed – as long as a secondary sanctions regime is not in place. The size of its telecommunications market gives the US a huge leverage to force the compliance of alternative suppliers, most of them located in Taiwan, South Korea, Japan, and sometimes Europe. These suppliers are not only dependent on the US market, but their production often depends also on the supply of components produced in the US. In this regard, it is telling that immediately after the American announcement, the German semiconductors company Infineon suspended its deliveries of products which include American components to Huawei Technologies.[41]

In this new context, decisions regarding Huawei and 5G infrastructure become even more political, beyond the complex question of network security and the question of the competitiveness of Huawei equipment. Because it is taking up so much political and media space, the controversy around Huawei is almost making us forget that

[40] "Cybersecurity Act," *European Commission* (2018), https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

[41] Cheng Ting-Fang and Lauly Li, "Germany's Infineon suspends US shipments to Huawei," *Nikkei Asian Review* (2019), https://asia.nikkei.com/Economy/Trade-war/Germany-s-Infineon-suspends-US-shipments-to-Huawei

there exist European solutions to the construction of the 5G infrastructure, giving the general public the impression that choosing Huawei is unavoidable. As of today, Ericsson and Nokia respectively hold 27% and 22% of the 2G/3G/4G gear market against 31% for Huawei, helped admittedly by the closure to Huawei of the US market.[42] In 2018, Ericsson even overtook Huawei according to IHS Markit, reaching a 29% world market share against 26% for Huawei. Both Nordic companies are very well positioned for 5G. Just like Huawei, these two European companies need supplies from the United States to deliver their offer of 5G equipment.[43]

But in contrast to Huawei, a European competitor like Ericsson invests much less in public relations. Relatively unnoticed by the media, it is already building 5G networks for operators in the US, South Korea, Saudi Arabia, and Australia – by April 2019, 18 public contracts had been signed.[44] The first commercial 5G rollouts in South Korea and with Verizon in the US are operating with Ericsson technology. In China, the Scandinavian OEM is active in many projects with Chinese operators from Qingdao harbor to trials on the Internet of Things. Likewise, in March 2019 Nokia announced the signing of a 30th commercial contract for 5G rollout, with an Austrian operator.[45] The Finnish OEM is active in Saudi Arabia, South Africa, the US, Egypt, Japan, Australia, Norway, Finland, South Korea, and Germany. Like Ericsson, Nokia is present in 5G in China, particularly in research and development, via contracts with China Mobile and Tencent.[46]

[42] "IHS Markit: Huawei Led Global 4G LTE Infrastructure Market which totalled $22.9B in 2018; China CAPEX bottoms out," *IEEE Communications Society Technology Blog* (2019), https://techblog.comsoc.org/2019/04/03/huawei-led-global-4g-lte-infrastructure-market-which-totalled-22-9b-in-2018/

[43] Shunsuke Tabeta and Takashi Kawakami, "US fight dethrones Huawei as top mobile equipment provider," *Nikkei Asian Review* (2019), https://asia.nikkei.com/Business/Business-trends/US-fight-dethrones-Huawei-as-top-mobile-equipment-provider

[44] "Live 5G networks and publicly announced 5G contracts," *Ericsson,* https://www.ericsson.com/en/5g/5g-networks/5g-contracts

[45] "Nokia celebrates 30th commercial 5G deal," *Nokia* (2019), https://www.nokia.com/about-us/news/releases/2019/03/28/nokia-celebrates-30th-commercial-5g-deal/

[46] "Nokia and China Mobile to set up joint AI*5G lab for further research using artificial intelligence and machine learning in 5G networks," *Nokia* (2018), https://www.nokia.com/about-us/news/releases/2018/07/06/nokia-and-china-mobile-to-set-up-joint-ai5g-lab-for-further-research-using-artificial-intelligence-and-machine-learning-in-5g-networks/ "Nokia and Tencent sign agreement to accelerate 5G webscale research and applications to benefit millions of Internet users in China," *Nokia* (2018), https://www.nokia.com/about-us/news/releases/2018/07/05/nokia-and-tencent-sign-agreement-to-accelerate-5g-webscale-research-and-applications-to-benefit-millions-of-internet-users-in-china/

IV

CONCLUSION AND RECOMMENDATIONS: 5G, A CRITICAL EUROPEAN INFRASTRUCTURE

In the absence of a single market for telecommunication frequencies within the EU and despite the efforts of the Commission to promote convergence of security standards, the progress of European countries has been uneven. For Europe, this creates a risk of falling behind, and even of strategic downgrading. European-scale equipment certification is a laudable step forward, but this is insufficient. Can Europe develop a less defensive, more proactive, and therefore more ambitious approach? With the saturation of the media space by the Huawei controversy, there is a risk that Europe will be distracted from an issue which is key to ensuring its place in a fast-changing international order. Indeed, the construction of the 5G infrastructure gives Europe an opportunity to consolidate its technological and industrial offering and build one of the tools for European sovereignty.

Consider 5G as a critical infrastructure working for European sovereignty

The advent of 5G is multiplying the risks inherent in the absence of European sovereignty. The protection of European data – and therefore the promotion of autonomy of political decision-making and the construction of an environment minimizing risks for companies – calls for choices which go far beyond the calculation of costs for operators and the immediate interests of consumers. The first of these choices is to reduce or balance dependency on outside suppliers. This is especially the case since the traditional influence exerted by the US through its suppliers is today compounded by the risk of a Sino-American duopoly or even the supremacy of China over the telecommunication sector. It is also important to realize that if interoperability between equipment providers exists (which comes at a cost), the division of Europe's 5G infrastructure between Huawei-equipped zones and zones supplied by other manufacturers undermines the strategic coherence of Europe between China and the United States.

Act in accordance with the precautionary principle

Because it is impossible for Huawei to demonstrate that it has no close and indelible links with the Chinese party state, there is an urgent need to keep this company away from risky infrastructures. The whole question is, of course, to determine the extent of the problem. In some cases, the company remains a useful spur to competition. The need to secure networks against the risk of sabotage means that there must never be reliance on a single supplier. If Europe is not capable of supporting its companies which still hold a large share of the world market, it must make a default choice by adding other non-European companies to them. They will all raise security issues, but none in an as uncontrollable a manner as Huawei.

Intensify defensive efforts

All flaws in 5G architecture are likely to be exploited by malicious actors. There is no Maginot line in the protection of interconnected networks. The training of qualified staff is a critical investment. The strengthening of human resources in the least well-provided member states is also important. The promotion of joint practices by the European Union must be supported by the member states most advanced in their 5G certification process. The sharing of R&D in network security must go further, as the data to be protected will not be concentrated at a few very specific points on European territory. The current European approach focused on administrative regulation and the certification of equipment should be the subject of an exchange of best practices with the American ally. Europe must also reach a conclusion on the administrative measures needed to manage the risk of 5G equipment in the longer term. It is clear that there is no technical answer today that will remain valid with certainty in 5 years, as the balance between offensive and defensive measures against telecommunication networks is by essence unstable.

Support an ecosystem favorable to technological competitiveness in Europe

In the case of 5G, European champions already exist. Huawei's price competition benefits European consumers and the public finances: the telecom operators low procurement costs compensate the high investments in broadband spectrum auctions. But this is also handicapping European gear suppliers. Without the

competition of Huawei, an intra-European consultation would be needed to build a market from a sufficient scale for the necessary investments to be profitable. Overall, Europeans can't avoid the question of the US market, and therefore of cooperation with American manufacturers such as Qualcomm, Broadcomm, and Nvidia to name a few. Other aspects may encourage the construction of a European ecosystem: equipment standards and regulation aspects; support for research and development; support for the emergence of European champions in the cloud; protection of OEMs against the risk of buyouts decreasing European industrial autonomy; or alternatively, new transatlantic industrial alliances. Protecting the European interest is inconceivable without robust investment in infrastructures, enabling European companies to expand.

ABOUT THE AUTHORS

Mathieu Duchâtel, Director of the Asia Program
Dr. Mathieu Duchâtel is Director of the Asia Program at Institut Montaigne since January 2019. Before joining the Institute he was Senior Policy Fellow and Deputy Director of the Asia and China Program at the European Council of Foreign Relations (2015-2018), Senior Researcher and the Representative in Beijing of the Stockholm International Peace Research Institute (2011-2015), Research Fellow with Asia Centre in Paris (2007-2011) and Associate Researcher based in Taipei with Asia Centre (2004-2007). He holds a Ph.D in political science from the Institute of Political Studies (Sciences Po, Paris). He has spent a total of nine years in Shanghai (Fudan University), Taipei (National Chengchi University) and Beijing and has been visiting scholar at the School of International Studies of Peking University in 2011/2012 and the Japan Institute of International Affairs in 2015.

François Godement, Senior Advisor for Asia, Institut Montaigne
François Godement is Senior Advisor for Asia to Institut Montaigne, Paris. He is also a non-resident senior associate of the Carnegie Endowment for International Peace in Washington, D.C., and an external consultant for the Policy Planning Staff of the French Ministry of Foreign Affairs. Until December 2018, he was the Director of ECFR's Asia & China program and a Senior Policy Fellow at ECFR. A long-time professor at France's National Institute of Oriental Languages and Civilisations and Sciences Po, he created Centre Asie IFRI at the Paris-based Institut Français des Relations Internationales (1985-2005), and in 2005 Asia Centre as an independent. He is a graduate of the Ecole Normale Supérieure de la Rue d'Ulm (Paris), where he majored in history, and a postgraduate student at Harvard University. In 1995 he co-founded the European committee of the Council for Security Cooperation in the Asia-Pacific (CSCAP), which he co-chaired until 2008. He has also been a member of the advisory board for the Europe China Academic Network (ECAN).

Acknowledgments

This project benefited from insights through research interviews conducted between January and April 2019 in France and Europe with representatives from the private sector and the administration who prefer to remain anonymous. Institut Montaigne is grateful for their time and intellectual contribution.

The information and views set out in this report are those of Institut Montaigne and do not necessarily reflect the opinions of the people and institutions mentioned above.

OUR PREVIOUS PUBLICATIONS

- 5G in Europe: Time to Change Gear! (mai 2019)
- Media polarization « à la française »? comparing the French and American ecosystems (mai 2019)
- Travailleurs des plateformes : liberté oui, protection aussi (mai 2019)
- Energie solaire en Afrique : un avenir rayonnant ? (février 2019)
- IA et emploi en santé : quoi de neuf docteur ? (janvier 2019)
- Cybermenace : avis de tempête (novembre 2018)
- Partenariat franco-britannique de défense et de sécurité : améliorer notre coopération, (novembre 2018)
- Sauver le droit d'asile (octobre 2018)
- Industrie du futur, prêts, partez ! (septembre 2018)
- La fabrique de l'islamisme (septembre 2018)
- Protection sociale : une mise à jour vitale (mars 2018)
- Innovation en santé : soignons nos talents (mars 2018)
- Travail en prison : préparer (vraiment) l'après (février 2018)
- ETI : taille intermédiaire, gros potentiel (janvier 2018)
- Réforme de la formation professionnelle : allons jusqu'au bout ! (janvier 2018)
- Espace : l'Europe contre-attaque ? (décembre 2017)
- Justice : faites entrer le numérique (novembre 2017)
- Apprentissage : les trois clés d'une véritable transformation (octobre 2017)
- Prêts pour l'Afrique d'aujourd'hui ? (septembre 2017)
- Nouveau monde arabe, nouvelle « politique arabe » pour la France (août 2017)
- Enseignement supérieur et numérique : connectez-vous ! (juin 2017)
- Syrie : en finir avec une guerre sans fin (juin 2017)
- Énergie : priorité au climat ! (juin 2017)
- Quelle place pour la voiture demain ? (mai 2017)
- Sécurité nationale : quels moyens pour quelles priorités ? (avril 2017)
- Tourisme en France : cliquez ici pour rafraîchir (mars 2017)
- L'Europe dont nous avons besoin (mars 2017)
- Dernière chance pour le paritarisme de gestion (mars 2017)
- L'impossible État actionnaire ? (janvier 2017)
- Un capital emploi formation pour tous (janvier 2017)
- Économie circulaire, réconcilier croissance et environnement (novembre 2016)
- Traité transatlantique : pourquoi persévérer (octobre 2016)
- Un islam français est possible (septembre 2016)
- Refonder la sécurité nationale (septembre 2016)
- Bremain ou Brexit : Europe, prépare ton avenir ! (juin 2016)
- Réanimer le système de santé - Propositions pour 2017 (juin 2016)

- Nucléaire : l'heure des choix (juin 2016)
- Un autre droit du travail est possible (mai 2016)
- Les primaires pour les Nuls (avril 2016)
- Le numérique pour réussir dès l'école primaire (mars 2016)
- Retraites : pour une réforme durable (février 2016)
- Décentralisation : sortons de la confusion / Repenser l'action publique dans les territoires (janvier 2016)
- Terreur dans l'Hexagone (décembre 2015)
- Climat et entreprises : de la mobilisation à l'action / Sept propositions pour préparer l'après-COP21 (novembre 2015)
- Discriminations religieuses à l'embauche : une réalité (octobre 2015)
- Pour en finir avec le chômage (septembre 2015)
- Sauver le dialogue social (septembre 2015)
- Politique du logement : faire sauter les verrous (juillet 2015)
- Faire du bien vieillir un projet de société (juin 2015)
- Dépense publique : le temps de l'action (mai 2015)
- Apprentissage : un vaccin contre le chômage des jeunes (mai 2015)
- Big Data et objets connectés. Faire de la France un champion de la révolution numérique (avril 2015)
- Université : pour une nouvelle ambition (avril 2015)
- Rallumer la télévision : 10 propositions pour faire rayonner l'audiovisuel français (février 2015)
- Marché du travail : la grande fracture (février 2015)
- Concilier efficacité économique et démocratie : l'exemple mutualiste (décembre 2014)
- Résidences Seniors : une alternative à développer (décembre 2014)
- Business schools : rester des champions dans la compétition internationale (novembre 2014)
- Prévention des maladies psychiatriques : pour en finir avec le retard français (octobre 2014)
- Temps de travail : mettre fin aux blocages (octobre 2014)
- Réforme de la formation professionnelle : entre avancées, occasions manquées et pari financier (septembre 2014)
- Dix ans de politiques de diversité : quel bilan ? (septembre 2014)
- Et la confiance, bordel ? (août 2014)
- Gaz de schiste : comment avancer (juillet 2014)
- Pour une véritable politique publique du renseignement (juillet 2014)
- Rester le leader mondial du tourisme, un enjeu vital pour la France (juin 2014)
- 1 151 milliards d'euros de dépenses publiques : quels résultats ? (février 2014)

- Comment renforcer l'Europe politique (janvier 2014)
- Améliorer l'équité et l'efficacité de l'assurance-chômage (décembre 2013)
- Santé : faire le pari de l'innovation (décembre 2013)
- Afrique-France : mettre en œuvre le co-développement
  Contribution au XXVI[e] sommet Afrique-France (décembre 2013)
- Chômage : inverser la courbe (octobre 2013)
- Mettre la fiscalité au service de la croissance (septembre 2013)
- Vive le long terme ! Les entreprises familiales au service de la croissance et de l'emploi (septembre 2013)
- Habitat : pour une transition énergétique ambitieuse (septembre 2013)
- Commerce extérieur : refuser le déclin
  Propositions pour renforcer notre présence dans les échanges internationaux (juillet 2013)
- Pour des logements sobres en consommation d'énergie (juillet 2013)
- 10 propositions pour refonder le patronat (juin 2013)
- Accès aux soins : en finir avec la fracture territoriale (mai 2013)
- Nouvelle réglementation européenne des agences de notation : quels bénéfices attendre ? (avril 2013)
- Remettre la formation professionnelle au service de l'emploi et de la compétitivité (mars 2013)
- Faire vivre la promesse laïque (mars 2013)
- Pour un « New Deal » numérique (février 2013)
- Intérêt général : que peut l'entreprise ? (janvier 2013)
- Redonner sens et efficacité à la dépense publique
  15 propositions pour 60 milliards d'économies (décembre 2012)
- Les juges et l'économie : une défiance française ? (décembre 2012)
- Restaurer la compétitivité de l'économie française (novembre 2012)
- Faire de la transition énergétique un levier de compétitivité (novembre 2012)
- Réformer la mise en examen Un impératif pour renforcer l'État de droit (novembre 2012)
- Transport de voyageurs : comment réformer un modèle à bout de souffle ? (novembre 2012)
- Comment concilier régulation financière et croissance :
  20 propositions (novembre 2012)
- Taxe professionnelle et finances locales : premier pas vers une réforme globale ? (septembre 2012)
- Remettre la notation financière à sa juste place (juillet 2012)
- Réformer par temps de crise (mai 2012)
- Insatisfaction au travail : sortir de l'exception française (avril 2012)
- Vademecum 2007 – 2012 : Objectif Croissance (mars 2012)

- Financement des entreprises : propositions pour la présidentielle (mars 2012)
- Une fiscalité au service de la « social compétitivité » (mars 2012)
- La France au miroir de l'Italie (février 2012)
- Pour des réseaux électriques intelligents (février 2012)
- Un CDI pour tous (novembre 2011)
- Repenser la politique familiale (octobre 2011)
- Formation professionnelle : pour en finir avec les réformes inabouties (octobre 2011)
- Banlieue de la République (septembre 2011)
- De la naissance à la croissance : comment développer nos PME (juin 2011)
- Reconstruire le dialogue social (juin 2011)
- Adapter la formation des ingénieurs à la mondialisation (février 2011)
- « Vous avez le droit de garder le silence… »
  Comment réformer la garde à vue (décembre 2010)
- Gone for Good? Partis pour de bon ?
  Les expatriés de l'enseignement supérieur français aux États-Unis (novembre 2010)
- 15 propositions pour l'emploi des jeunes et des seniors (septembre 2010)
- Afrique - France. Réinventer le co-développement (juin 2010)
- Vaincre l'échec à l'école primaire (avril 2010)
- Pour un Eurobond. Une stratégie coordonnée pour sortir de la crise (février 2010)
- Réforme des retraites : vers un big-bang ? (mai 2009)
- Mesurer la qualité des soins (février 2009)
- Ouvrir la politique à la diversité (janvier 2009)
- Engager le citoyen dans la vie associative (novembre 2008)
- Comment rendre la prison (enfin) utile (septembre 2008)
- Infrastructures de transport : lesquelles bâtir, comment les choisir ? (juillet 2008)
- HLM, parc privé
  Deux pistes pour que tous aient un toit (juin 2008)
- Comment communiquer la réforme (mai 2008)
- Après le Japon, la France…
  Faire du vieillissement un moteur de croissance (décembre 2007)
- Au nom de l'Islam… Quel dialogue avec les minorités musulmanes en Europe ? (septembre 2007)
- L'exemple inattendu des Vets
  Comment ressusciter un système public de santé (juin 2007)
- Vademecum 2007-2012
  Moderniser la France (mai 2007)

- Après Erasmus, Amicus
  Pour un service civique universel européen (avril 2007)
- Quelle politique de l'énergie pour l'Union européenne ? (mars 2007)
- Sortir de l'immobilité sociale à la française (novembre 2006)
- Avoir des leaders dans la compétition universitaire mondiale (octobre 2006)
- Comment sauver la presse quotidienne d'information (août 2006)
- Pourquoi nos PME ne grandissent pas (juillet 2006)
- Mondialisation : réconcilier la France avec la compétitivité (juin 2006)
- TVA, CSG, IR, cotisations…
  Comment financer la protection sociale (mai 2006)
- Pauvreté, exclusion : ce que peut faire l'entreprise (février 2006)
- Ouvrir les grandes écoles à la diversité (janvier 2006)
- Immobilier de l'État : quoi vendre, pourquoi, comment
  (décembre 2005)
- 15 pistes (parmi d'autres…) pour moderniser la sphère publique
  (novembre 2005)
- Ambition pour l'agriculture, libertés pour les agriculteurs (juillet 2005)
- Hôpital : le modèle invisible (juin 2005)
- Un Contrôleur général pour les Finances publiques (février 2005)
- Les oubliés de l'égalité des chances (janvier 2004 - Réédition septembre 2005)

For previous publications, see our website:
www.**institutmontaigne.org/en**

INSTITUT
MONTAIGNE

ABB FRANCE
ACCURACY
ADIT
AIR FRANCE - KLM
AIRBUS GROUP
ALLEN & OVERY
ALLIANZ
ALVAREZ & MARSAL FRANCE
ARCHERY STRATEGY CONSULTING
ARCHIMED
ARDIAN
ASTRAZENECA
A.T. KEARNEY
AUGUST DEBOUZY
AXA
BAKER & MCKENZIE
BANK OF AMERICA MERRILL LYNCH
BEARINGPOINT
BESSÉ
BNI FRANCE ET BELGIQUE
BNP PARIBAS
BOLLORÉ
BOUGARTCHEV MOYNE ASSOCIES
BOUYGUES
BPCE
BRUNSWICK
CAISSE DES DEPÔTS
CAPGEMINI
CAPITAL GROUP
CARBONNIER LAMAZE RASLE & ASSOCIÉS
CAREIT
CARREFOUR
CASINO
CHAÎNE THERMALE DU SOLEIL
CHUBB
CIS
CISCO SYSTEMS FRANCE
CMA GCM
CNP ASSURANCES
COHEN AMIR-ASLANI
COMPAGNIE PLASTIC OMNIUM
CONSEIL SUPÉRIEUR DU NOTARIAT
CORREZE & ZAMBEZE
CRÉDIT AGRICOLE
CRÉDIT FONCIER DE FRANCE
D'ANGELIN & CO. LTD
DENTSU AEGIS NETWORK
DE PARDIEU BROCAS MAFFEI
DRIVE INNOVATION INSIGHTS - DII
EDF
EDHEC BUSINESS SCHOOL
ELSAN
ENGIE
EQUANCY
EURAZEO
EUROGROUP CONSULTING
EUROSTAR
FIVES
FONCIÈRE INEA
FONDATION ROCHE
GALILEO GLOBAL EDUCATION FRANCE
GIDE LOYRETTE NOUEL
GOOGLE
GRAS SAVOYE
GROUPAMA
GROUPE EDMOND DE ROTHSCHILD
GROUPE M6
GROUPE ORANGE
HAMEUR ET CIE
HENNER
HSBC FRANCE
IBM FRANCE
IFPASS
ING BANK FRANCE
INSEEC
INTERNATIONAL SOS
IONIS EDUCATION GROUP
ISRP
JEANTET ASSOCIÉS
KANTAR
KPMG S.A.
LA BANQUE POSTALE
LA PARISIENNE ASSURANCES
LAZARD FRÈRES
LINEDATA SERVICES

SUPPORT INSTITUT MONTAIGNE

INSTITUT
MONTAIGNE

LIR
LIVANOVA
LOXAM
LVMH - MOËT-HENNESSY - LOUIS VUITTON
MACSF
MALAKOFF MÉDÉRIC
MAREMMA
MAZARS
MCKINSEY & COMPANY FRANCE
MÉDIA-PARTICIPATIONS
MEDIOBANCA
MERCER
MERIDIAM
MICHELIN
MICROSOFT FRANCE
MITSUBISHI FRANCE
NEHS
NATIXIS
NESTLÉ
OBEA
ODDO BHF
ONDRA PARTNERS
OPTIGESTION
ORANO
ORTEC GROUP
PAI PARTNERS
PIERRE ET VACANCES
PRICEWATERHOUSECOOPERS
PRUDENTIA CAPITAL
RADIALL
RAISE
RAMSAY GÉNÉRALE DE SANTÉ
RANDSTAD
RATP
RELX GROUP
RENAULT
REXEL
RICOL, LASTEYRIE CORPORATE FINANCE
RIVOLIER
ROCHE
ROLAND BERGER
ROTHSCHILD MARTIN MAREUL
SAFRAN
SANTÉCLAIR
SCHNEIDER ELECTRIC
SERVIER
SGS
SIA PARTNERS
SIACI SAINT HONORÉ
SIEMENS
SIER CONSTRUCTEUR
SNCF
SNCF RÉSEAU
SODEXO
SOFINORD-ARMONIA
SOLVAY
SPRINKLR
SUEZ
SYSTEMIS
TECNET PARTICIPATIONS SARL
TEREGA
THE BOSTON CONSULTING GROUP
TILDER
TOTAL
UBER
UBS FRANCE
VEOLIA
VINCI
VIVENDI
VOYAGEURS DU MONDE
WAVESTONE
WENDEL
WILLIS TOWERS WATSON
WORDAPPEAL

SUPPORT INSTITUT MONTAIGNE

INSTITUT
MONTAIGNE

INSTITUT
MONTAIGNE

THERE IS NO DESIRE MORE NATURAL THAN THE DESIRE FOR KNOWLEDGE

Europe and 5G: the Huawei Case

What choices for 5G infrastructure in Europe? By taking on a controversial dimension, the Huawei case reveals crucial strategic issues for Europe, between China and the United States. 5G is a critical infrastructure that will transform economic activity, generating a generational leap for some companies, penalizing actors outside its deployment, and raising serious challenges in terms of data protection and national security.

But Europe is moving in a dispersed order and the saturation of the media space by the Huawei controversy is diverting European energies away from an essential stake for Europe's place in a changing international order. On the one hand, it is necessary to act according to the safety first principle against Huawei, a company that has been unable to demonstrate its lack of deep links with the core of China's state apparatus. On the other hand, the construction of 5G networks is an opportunity to consolidate a technological and industrial offer in Europe and to build a tool for European sovereignty.

This note from Institut Montaigne's Asia Program analyzes the risks linked to the Huawei 5G offer for Europe and underlines the political importance of supporting an ecosystem that is favorable to Europe's technological competitiveness.

Follow us on:

Sign up for our weekly newsletter on:

www.institutmontaigne.org/en

Institut Montaigne
59, rue La Boétie - 75008 Paris
Tél. +33 (0)1 53 89 05 60
www.institutmontaigne.org

ISSN 1771-6756
JUNE 2019