PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

POLICY PAPER

No. 1 (171), January 2019 © PISM

China and the Challenges of the Fourth Industrial Revolution: Value Chains, 5G, and Emerging Markets

Marcin Przychodniak

China has identified the ongoing digital revolution as its first opportunity in modern times to compete with other international actors, especially the U.S. The competition serves as the driving force for enhancing innovation and finding new sources of growth for the Chinese economy. The advantage of technological development is that it will allow China to become a "major cyber power," introduce its own technological standards worldwide, raise its position in global value chains, and influence the world economy. But the process is seriously challenged by the change in China's relations with the U.S., concerns in the EU about Chinese investments as well as domestic centralisation of power.

The end of the Cold War happened in parallel to the period of China's continuous growth, expanding trade and investment relations, and—as a result—finally (in the 2000s) rising to the status of the principal competitor of the United States. As long as cooperation with the U.S. served China's interests, the People's Republic of China (PRC) refrained from open rivalry with the U.S. The Chinese authorities tried to popularise ideas like a "new type of great power relations[1]" (*xin xing da guo guanxi*) to describe bilateral contacts arguing that China and the U.S. are two big global powers. China's policy changed when Xi Jinping became the PRC chairman in 2013. Since then, he has centralised his power, promoted ideas of changing the global order, and announced the Belt and Road Initiative (BRI). His policy has been aimed to compete with U.S.-led ideas and initiatives. All of his tactics are also used in a domestic narrative aimed at strengthening nationalistic pride, symbolised by the slogan the "great rejuvenation of the Chinese nation" (*zhonghua minzu weida fuxing)*.[2] This change in foreign policy was based on clear Communist Party of China (CPC) analysis that if China continued its conservative approach and tried to adjust to the status quo, the country would not be able to develop its resources and, in the long term, compete as an equal with the U.S. Since

[1] For the first time, this slogan was used by Chairman Xi during a meeting with U.S. President Barack Obama in June 2013 and was intended to serve as a new definition of an equal relationship between the two powers. It has never been precisely defined by China nor was it acknowledged by the Obama administration.

[2] This is one of the slogans in the CPC narrative used, i.a., by Chairman Jiang Zemin and popularised during Xi's term. Parallel to "Chinese dream," it symbolises the Chinese nation regaining its international position after a period between 1839 and 1949 remembered in China as a time of humiliation by "Western powers." The CPC's main goal is to restore the Chinese nation to the position it believes it deserves on the international arena. The logic of the political process is essentially revanchist.

the usual drivers of growth in China (export growth, low-cost labour, and investment) were also running low, and with the financial crisis in the West proving the limits of external demand, the need for economic reforms became crucial.

The "fourth industrial revolution,[3]" as it is dubbed, seems to be a perfect opportunity for China to create for itself innovation-led development and growth in high-tech sectors. China has always held the U.S. in esteem as the inventor of the internet, achieved during the "third industrial revolution," and U.S. superiority in business, regulatory institutions, and technologies. China decided to create its own spheres to dominate and technological advantages. Introduced in May 2015, the "Made in China 2025" strategy (together with "Internet +")[4] was a clear example of this mindset. The U.S. resignation from formal control (though never used) of the Internet Assigned Numbers Authority (IANA)[5] was the first opportunity for China to strengthen its position in the digital industry and internet management.

The New Technological Revolution: China and the Internet

For Chinese leadership, now is the first chance in modern times to reverse what it views as a historical "process of humiliation" to speed up development, projected to end in 2049 (the 100th anniversary of the founding of the PRC), and to become "a leader among the world's manufacturing powers." The goal is to regain the status of a standard-setter, which China asserted centuries ago as the probable inventor of printing, paper, gunpowder, and numerous other inventions and technology.

The phrase, a "new round of technological revolution" (*xin yi lun jishu geming*; a term associated with Rifkin's "third industrial revolution,"[6] Schwab's "fourth industrial revolution" but first and foremost based on Toffler's ideas of different types of societies[7]) is the period presented by Chinese experts as a remarkable chance for China to acquire superpower status without a military conflict. A state-driven policy (applied in conventional sectors for the last 40 years), with government procurement, subsidies, and the involvement of large, state-owned enterprises,[8] seems to be the most successful mechanism for this. The Chinese authorities define artificial intelligence (AI), the "Internet of things" (IoT), and telecommunications as the main elements of its own technological revolution. These tools should help China secure "uninhabited areas" (*wurenqu*), that is, technological domains not dominated by the U.S. so far, and ensure China's superiority as a "major cyber power" (*wangluo qiangguo).*[9]

According to Xi, the main aspects of this technological revolution are to defend the interests of the people (*renmin liyi*) and the country's security (*guojia anquan*). In his official speeches, he has often instructed the CPC and state administration that AI is the core of China's technological development.[10] He argues that AI facilitates growth and economic reform, and has an important impact on the society. Xi also underscores that AI will influence the CPC's methods of governance, such as facilitating the achievement of goals in

[3] A term included in the book by K. Schwab. The main characteristics of the "fourth industrial revolution" are a fusion of technologies and emerging breakthroughs in robotics, AI, nanotechnology, and biotechnology. See: K. Schwab, *The Fourth Industrial Revolution,* World Economic Forum, 2016.

[4] A plan to apply internet and information technologies to conventional industries was included in the Government Work Report by Li Keqiang in March 2015.

[5] Internet Assigned Numbers Authority (IANA) is a function of the Internet Corporation for Assigned Names and Numbers (ICANN), which oversees global IP address allocations, among other tasks.

[6] "Kexue wang. Xin yu lun jishu geming dui zhongguo tiaozhan dayu jiyu geming" [Science network. A new round of technological revolution brings more challenges for China than opportunities], China Academy of Sciences, 18 January 2018, www.casad.cas.cn.

[7] See: H.Tofler, A. Tofler, *The Third Wave*, Bantam Books, 1980.

[8] Huang Qixuan, "Daguo quanli jingzheng ruhe yinfale jishu geming" [How competition between big powers triggers technological revolution], *The Paper,* 19 June 2018.

[9] E. Kania, S. Sacks, P. Triolo, G. Webster, "China's Strategic Thinking on Building Power in Cyberspace," *New America*, 25 September 2017, www.newamerica.org; for the original text, see: CAC Theoretical Studies Centre, "Shenru guanche Xi Jinping zong shuji wangluo qiangguo zhanlüe sixiang zhashi tuijin wangluo anquan he xinxi hua gongzuo" [Deepening the implementation of General Secretary Xi Jinping's strategic thinking on building China into a cyber superpower: steadily advancing cybersecurity and informatisation work], *Qiushi,* 15 September 2017, www.qstheory.cn.

[10] "Xi Jinping: tuidong wo guo xinyidai rengongzhineng jiankang fazhan" [Xi Jinping: promotion of the development of a new AI generation], *Xinhua*, 31 October 2018, xinhua.com.

education, healthcare, transportation, and housing. Finally, AI will enable government to better assess the exact needs of society and use its resources more efficiently to reform China's pension, healthcare, and education systems. AI though—and these are not Xi's words—will also provide the CPC with better control over society by giving it access to data on people's priorities, behaviour, and opinions, in one case all combined into a digitalised scoring and evaluation system already in development.

The internet in general is a key instrument in the fourth industrial revolution. Zhuang Rongwen, president of the Cyberspace Administration of China (CAC), recently described the country's strategy towards the internet in party magazine *Qiushi.*[11] Since the internet is an important "ingredient" in the technological revolution, it should be placed under strict ideological and political control. Zhuang admits that "whoever masters the internet holds the initiative of the era and whoever does not take the internet seriously will be cast aside by the times."[12] Although such a metaphor implies a serious rivalry between China and the United States, CAC's president—in parallel with Xi's recent messages on the need to cooperate with the U.S. on technology—leaves some space for other partners under "collaborative cyberspace."

The significance of China's involvement in the "new round of the technological revolution" makes it crucial for the CPC to keep control over the state's development process. Xi's leadership and his efforts to maintain party integrity are fundamental for his policy in the second term. So, it is mainly the CPC, not tech leaders, private enterprises, or research institutions, that is the driving force behind China's success in the "new round of the technological revolution."

Challenges[13]

China's ambitious plans (with AI, IoT, and 5G[14]) within the fourth industrial revolution are currently seriously challenged in both the external and internal dimensions. First and foremost is the negative change in U.S. policy towards China. It is visible not only in the trade disputes[15] but also in new export regulations on vital components[16] and restrictions on investment in the IT sector (the screening mechanism and reform of the Committee on Foreign Investment in the United States), as well as in restrictions in access of Chinese students and researchers to U.S. universities (due to visa limits). The U.S. is constantly repeating its stance that China needs to change its economic policy, especially in terms of state subsidies for Chinese companies, access to its market, and cybersecurity. The U.S. is also in the avant-garde of the opposition to the involvement of Chinese companies in 5G infrastructure development, not only asking foreign partners to stop cooperation with Chinese high-tech global enterprises like Huawei but also enacting its own restrictions.[17] The Chinese interest in 5G to date had already raised security concerns among several U.S. partners. Their main concern is that Chinese companies may gain the ability to control critical infrastructure responsible for the functioning of transport, education, healthcare, and energy. Access to sensitive data and the possibility of technical control might be used in the interests of the Chinese state. The so-called "five eyes"[18] countries (New Zealand, U.S., Australia, UK, and Canada) have decided to exclude Huawei

[11] Zhuang Rongwen, "Scientifically Understanding the Natural Laws of Online Communication, Striving to Boost the Level of Internet Use and Network Governance," *New America,* 24 September 2018, www.newamerica.org; See original here: Zhuang Rongwen, "Kexue renshi wangluo chuanbo guilu nuli tigao yong wang zhi wang shuiping," *Qiushi*, 16 September 2018, www.qstheory.cn.
[12] Zhuang Rongwen, *op. cit.*
[13] Part of the analysis is based on the discussion at the European China Economic Policy Workshop in MERICS, held in October 2018.
[14] 5G is a next-generation mobile communications standard. In comparison to its predecessors (4G, 3G, 2G) it provides higher speed, energy savings, higher system capacity, and allows users to create more sophisticated networks and data exchanges.
[15] J. Szczudlik, D. Wnukowski, "China grapples with changing U.S. trade policy," *PISM Bulletin,* 17 October 2018, no. 142 (1213), www.pism.pl.
[16] One of the biggest producers of surveillance equipment, Hikvision, suffered a huge loss in share value due to its dependence on microchips from Intel, Nvidia, and Ambarella. See: E. Feng, "Chinese surveillance group faces crippling U.S. ban," *Financial Times*, 18 November 2018, www.ft.com.
[17] J. Horowitz, "Huawei CFO Meng Wanzhou arrested in Canada, faces extradition to United States," *CNN,* 6 December 2018, www.cnn.com.
[18] The "five eyes"—the U.S., Australia, New Zealand, Canada, and the UK—are part of the UK-U.S. agreement signed in the 1940s that encompasses cooperation on signals intelligence.

from 5G.[19] Japan recently decided to ban Huawei and ZTE from public procurement and discouraged operators from 5G cooperation with Chinese partners. Softbank, a Japanese holding company that includes a mobile carrier, withdrew Huawei equipment from its 4G network and placed orders for 5G equipment from Nokia and Ericsson.

To rid itself of its perception as a "technological colony" (*jishu zhimin),* China tries to speed up its technological advances in designing and producing Chinese-made microchips and a computer operating system. The state programmes devoted to microchip production have succeeded in the development of devices used, for example, in the civil-aviation sector.[20] But the level of China-made technological solutions is still very low, which renders China vulnerable to U.S. competition.[21]

Next in importance is the external challenge of the change in EU policy towards China symbolised by speeding up work on the investment-screening mechanism.[22] Although the policies of individual EU Member States towards cooperation with China differ (several countries including Spain, Portugal, Greece, and Hungary pursue a positive approach towards working with China), the general European trend—due to the importance of the size of the EU market and the European Commission's competences in trade and investment—is worrying for China. The most important partners from the perspective of the "technological revolution" and EU institutions—France, Germany, and the UK—are no longer as positive towards China, especially in mergers and acquisitions of companies in the IT, robotics, and high-tech sectors.

The external challenges are just one part of the picture. Equally important is the range of internal factors that influence policymaking on economic reforms. China's economic policy is orchestrated directly by Xi Jinping, who took on unprecedented control especially by chairing leading central commissions (for financial and economic affairs and for comprehensively deepening reform). New development guidelines were introduced in Xi's speech at the 19th CPC National Congress in 2017. This was in response to the needs of the Chinese "middle class" and aimed at environmental protection, increasing innovation, and improving healthcare ("people-centred philosophy of development").[23] China's level of GDP growth seems not that important anymore. Cities and provinces are supposed to follow sophisticated policy supporting the development based on high-tech and innovation. Such a change from "high speed" to "high quality" growth has created confusion among local governments. New goals come from the central level and the local authorities are obliged to abide by them even though they sometimes are opposite their needs. At the same time, they also can be held accountable if they do not respond to the needs of their local populations.

The numerous inspections from different institutions, ministries, and the National Supervisory Commission constrain the decision-making of the local authorities, who constantly try to figure out the will of the central leadership and avoid a negative evaluation by the party. But then the circle closes: officials avoid decisions, but that lack of action makes them vulnerable to actual persecution.

The centralisation of power by Xi has not only reduced the efficiency of the local governments but also enhanced the subordination of private businesses to the CPC.[24] The most prominent cases of Chinese

[19] In July 2018, there was a meeting in Canada of senior intelligence officers from these countries, in part to discuss ways to confront China's cyber activities. See: C. Uhlmann, "Secret meeting led to the international effort to stop China's cyber espionage," *Financial Review*, 13 December 2018, www.afr.com.

[20] The X86 devices based on Chinese *Longxin* microchips are used, e.g., in Air China ticket sales systems.

[21] The U.S. Department of Commerce decided to stop cooperation between American companies and chipmaker Fujian Jinhua Integrated Circuit. The Chinese company is accused of stealing trade secrets from its U.S. rivals. The company was involved in state-sponsored projects to build microchips. See: "Chinese chipmakers brace for next US crackdown," *Asian Nikkei,* 2 November 2018, www.asian.nikkei.com.

[22] On 20 November 2018, the Austrian presidency reached a provisional agreement with European Parliament representatives on an EU framework for screening foreign direct investment. See: "Screening of investments: political agreement reached on an EU framework," *European Council,* 20 November 2018, www.consilium.europa.eu; P. Blenkinsop, "EU reaches provisional deal on screening foreign investments," *Reuters*, 20 November 2018, www.reuters.com.

[23] Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," *Xinhua*, 3 November 2017, www.xinhuanet.com.

[24] Wang Xiangwei, "China's vow to help private firms is plausible—but desperate, too," *South China Morning Post*, 17 November 2018, www.smcp.com.

private and global investment companies forced to follow party regulations in their investment policies include CEFC, the Wanda Group, and HNA.[25]

Party-controlled state capitalism enforced by the CPC also has a negative impact on research and development (R&D), which can succeed only through the close cooperation of businesses and research institutions.[26] Independent think-tanks are harassed (e.g., Unirule, a pro-market and constitutional democracy-oriented think-tank, was evicted without notice from its Beijing offices in 2018) and the ability to freely conduct academic research is limited. Academics are increasingly afraid of freely discussing issues and sometimes their passports are held by the institutions where they work.[27] Although China for many years has claimed to have the most new patents, it has not succeeded in implementing them.[28]

Countermeasures[29]

In order to deal with the challenges, the Chinese authorities decided to focus on specific aspects of the development plans in areas in which the country is already leading or has the potential to be number one. There are three significant areas. The first is cooperation with technologically less-developed markets in regions such as the Middle East, Africa, Southeast Asia, Central Europe, the Balkans, and Latin America. The aim is to focus on introducing into those markets Chinese brands and standards, as well as extend political influence. The second is telecommunications, especially 5G-technology development. The third is to advance Chinese standards and its companies in IT value chains, with specialisation in certain sectors.

On less-developed markets, the idea is to create interdependencies and use capital to foster cooperation. China is about to utilise its established market champions in selected niches[30] such as drones or surveillance equipment. The "Digital Silk Road" was established as a dedicated part of the BRI. To support it, numerous instruments are in use. China has delivered hardware and equipment to developing countries (about 35 states[31]) and although that has created strong economic links it is also questionable from the partner's security perspective. Along with this kind of cooperation goes attempts to transfer values compatible with the Chinese concept of the freedom of information. A Freedom House report identified how Chinese officials have held sessions on these issues with 36 of 65 countries assessed.[32]

5G is currently perceived by the Chinese as a "mark of quality" and convenient tool to gain an advantage in terms of technology competition and market share.[33] The development of 5G infrastructure is considered by the Chinese authorities to be similar to the invention of the internet by the U.S. in the 1980s. China already dominates 4G services globally in terms of the number of users and technologies. It feels it has a natural opportunity to become a major competitor and supplier of 5G technology with higher speeds, reduced latency, and energy savings. The main Chinese company responsible for 5G development is Huawei (see Table 1) which established B2B partnerships in Europe, Asia, and other world regions (around 25 5G

[25] Zhou Xin, "China signals big economic shift in economic course due to US trade war headwinds," 2 November 2018, www.scmp.com.

[26] On 12 October 2018, the International Standards Organisation accepted Alibaba's proposal for a standard on big data security and a privacy process. Now, it will go through the ISO process, which means it might be adopted.

[27] Based on a presentation at the European China Economic Policy Workshop in MERICS, held in October 2018.

[28] Lulu Chen, "China claims more patents than any country—most are worthless," *Bloomberg*, 26 September 2018, www.bloomberg.com.

[29] Part of the analysis is based on the discussion at the European China Economic Policy Workshop in MERICS, held in October 2018.

[30] Chinese drone manufacturer DJI is reported to control up to 70% of the global drone market. China is also a leader in surveillance technology, with Hangzhou Hikvision Digital Technology controlling over 20% of the global market. See: "Is China a global leader in research and development?," *China Power*, 31 January 2018. https://chinapower.csis.org.

[31] The equipment was delivered, i.a., to Tonga (in 2014), Malawi (in 2018), Pakistan (in 2017), Belarus, Serbia, Laos, Sri Lanka, Nigeria, Mauritius, Seychelles, and Vanuatu. See: E. Thomas, "As the West warns of Chinese cyber spies, poorer nations welcome gifts with open arms," *The Wired*, 11 June 2018, www.wired.co.uk.

[32] "Chinese style 'digital authoritarianism' grows globally: study," 31 October 2018, www.straittimes.com.

[33] B. Perez, Li Tao, "'Made in China 2025': How 5G could put China in charge of the wireless backbone and ahead of the pack," *South China Morning Post*, 15 October 2018, www.scmp.com.

MoUs with operators[34]). China wants to provide the technology and keep its influence on the future development and maintenance of critical infrastructure connected with 5G. The International Telecommunication Union, a specialised UN agency headed by Chinese official Zhao Houlin (re-elected in November 2018), is at the same time the main global agency overseeing the worldwide development of 5G and may be an important part of the Chinese plans. Huawei has the most 5G intellectual property rights among the Chinese entities[35] (but still fewer than U.S. companies).

In order to minimise the costs of access to the U.S. or European technologies, China is trying to take control of whole production chains in certain sectors and products. In the e-mobility sector, especially electric vehicle batteries, it already dominates the international market. China declares it is opening up its market to foreign partners but is doing so in exchange for including made-in-China products in the production processes of world-known brands. Such a *modus operandi* was applied, for example, to a deal concerning a BMW factory in Shenyang. The German automaker was allowed to operate on the Chinese market without a joint venture with a Chinese company, required under previous rules. In exchange, China expects its own products to be included in the production process to gain recognition of them as used by BMW. Another example is Google's Dragonfly project, characterised as a "compromise" for access to the Chinese market. It was to be a censored search engine set up in a joint venture with an unnamed Chinese company.[36] Ordinary access to Google's products has been blocked in China since 2012.

China's already difficult relations with the U.S. and increasingly troublesome ties with some EU Member States (at least from the perspective of technology profits) has made it intensify its relations with other partners, such as Israel, Canada, and Turkey but also to some extent with Japan.[37] The sectors of cooperation range from IT applications to environmental solutions to e-mobility vehicles, and in each China tries to grab every opportunity to strengthen its dominant position. It also tries to influence the policies of its partners' AI strategies, which, in the Israel case favours government support for industry and civil-military collaboration. It is also one of the solutions to—at least partially—replace the delivery channels of, for example, microchips from U.S. and European companies.[38]

The internal challenges are much harder to overcome. The CPC is aware of its economy's stagnation and the negative effects of the centralisation of power on technology development. The main problem is impossible to resolve: the CPC has to keep its supervision to maintain the current political order. So, the Chinese authorities are now trying to balance the problems without touching the issue directly. They have managed to decrease and regulate the number of central inspections on local governments: the approval of the State Council to carry out an inspection is now required. The appraisal for state-owned enterprises is combined with messages of support for private enterprises.

Conclusions for Poland and the EU

Poland has recently experienced a period of rich political exchange with China, culminating in the signing of a comprehensive strategic agreement during Xi's state visit to Poland in 2016. There are also signals of China's interest in high-tech cooperation with Poland. A good example is the noticeable presence of Chinese companies from the IT sector, such as Lenovo, ZTE, and Xiaomi on the Polish market. But the difference in the level of innovation and investment possibilities between Poland and other European

[34] Different sources mention several numbers of agreements on 5G signed by Huawei with operators. Anyhow, it still amounts to fewer than Sweden's Ericsson and Finland's Nokia. It is, however, ahead in 4G infrastructure, which might become an advantage. See: E. Auchard, Sijia Jiang, "China's Huawei set to lead global charge to 5G networks," *Reuters*, 23 February 2018, www.reters.com; "Zhongguo 5G yanfa jinru quanqiu lingxian tidui," *People's Daily*, 9 November 2018, www.people.com.cn; "Yu Huawei chengwei 5G hezuo huoban de guojia you naxie" (Who are Huawei's partners?), *Elecfans*, 14 December 2018, elecfans.com.

[35] B. Perez, Li Tao, *op. cit*.

[36] It seems that due to internal disputes between Google employers and the board over the differences on Dragonfly, the whole project was suspended. See: R. Gallagher, "Google's Secret China Project 'Effectively Ended' After Internal Confrontation," *The Intercept*, 17 December 2018, www.theintercept.com.

[37] Geely Automobile Holdings started talks with Toyota on acquiring gasoline-electric technology.

[38] "Obscure Chinese firm Wingtech Technology Co will buy Dutch chipmaker Nexperia for US$3,6 billion," *South China Morning Post*, 26 October 2018, www.scmp.com.

countries, such as Germany or the UK, makes Poland less attractive to China in terms of technological cooperation. Nevertheless, certain aspects, such as 5G infrastructure, are definitely worth noticing from China's perspective. Huawei is also aware that Samsung, Ericsson, and Nokia have already established R&D centres in Poland and the Chinese company does not want to remain behind its competitors. During the Shanghai International Expo in November, the Polish secretary of state attached to the office of the prime minister, Marek Suski, also announced the near certainty that Huawei would open an R&D centre near Warsaw.

Huawei is already trying to use this opportunity. During its 14 years on the Polish market, it has become a leader in terms of retail sales of smartphones[39] and an important partner to operators. Huawei's office in Poland is also the company's CEE and Nordic headquarters. In December 2018, it opened its first flagship store in one of Warsaw's shopping malls. The company is very much interested in 5G infrastructure, especially cooperation with mobile operators in providing equipment for the network. Although major operator Orange has broken ties with Huawei in France it is conducting 5G trials with the Chinese company in Gliwice, Poland. What is more, TMobile has just started its first 5G trial run in Warsaw and is cooperating closely with Huawei. It is worth mentioning that the Chinese company started a public relations campaign touting its cooperation in Poland. Huawei supported Congress 590,[40] a technology event in Poland, invited Polish journalists to participate in a study visit to its facilities in Italy, and carried out seminars at Poland's Office of Electronic Communications (the national regulator) on the technological and commercial aspects of implementing 5G technology.

Although China's development plans may sound like a commercial opportunity based on innovative solutions and competitive prices, they have raised a lot of concerns, especially from the security perspective. The cooperation with Huawei and other Chinese high-tech companies is problematic due to their legal and personal subordination to the CPC's political interests. An interesting recent example is an espionage case in Poland.[41] Also, there have been reports recently of Chinese technical devices being used for secondary purposes, such as chips that were gathering data from Apple and Amazon devices, and the hardware at African Union headquarters,[42] as well as hacking in the Czech Republic,[43] and China Telecom's use of point-of-presence.[44] Access to infrastructure (in both 4G and 5G systems) gives the operator and equipment provider the ability to acquire data and information on users, institutions, and enterprises. Poland needs to finally develop an official, clear, and restrained position towards cooperation with Chinese IT and telecommunication enterprises, especially in the context of 5G and critical infrastructure. The engagement of Chinese enterprises needs to be transparent and Polish state institutions' full control over access to databases and data flow must be ensured. Lacking that, these companies may be excluded from cooperation on critical infrastructure. This is especially important since the development of 5G infrastructure in Poland is worth about $7 billion (plus the cost of frequencies at auction).[45] Potential

[39] According to IDC analysts, Huawei's share of the Polish smartphone market rose above 32% in Q2 2018 and outstripped Samsung, which sold the most smarthpones in 1Q 2018; M. Szewczak, "Huawei numer 1 w Polsce w II kw" [Huawei a number one in Poland in 2Q], *GSMOnline*, 2 August 2018, www.gsmonline.pl

[40] Congress 590 is a yearly conference organised in Jasionka near Rzeszów to promote Polish technological solutions and exchange information between politicians, businesspeople and experts. Its name comes from the Polish product code (590). It is organised by the foundation linked to the National Bank of Poland, with donations by state-owned companies and perceived as a government-backed initiative.

[41] In January, a Polish citizen and a Chinese executive working for Huawei Poland were authorised to be arrested by a court in Poland on grounds of possible espionage.

[42] The African Union headquarters in Addis Ababa was financed and built by Chinese contractors for around $200 million. In January 2018, the French newspaper *Le Monde* published an investigation on the alleged transfer of data from servers located in the headquarters to Shanghai, China. See: D. Cave, "The African Union headquarters hack and Australia's 5G network," Australian Strategic Policy Institute, 12 July 2018, www.aspistrategist.org.au.

[43] According to the information, between 2014 and 2016, Chinese hackers entered the network of the Czech Ministry of Foreign Affairs. The attack happened at the same time as a Russian attack but they were not coordinated. However, both sides knew about each other, monitored their illegal activity, and tolerated each other's presence. O. Kundra, "EU under cyberattack by Russia and China," *Re:Baltica*, 18 October 2018, en.rebaltica.lv.

[44] Since February 2016, much traffic from, e.g., Italy or Canada were directed through China, which created the possibility to intercept the data. See: C. Cimpanu, "China has been hijacking the vital internet backbone of western countries," 26 October 2018, zdnet.com.

[45] "Chiński problem sieci piątej generacji" [Chinese problem of fifth-generation network], *Puls Biznesu*, 2 June 2018, www.pb.pl

contractors are already counting on government financial involvement due to a lack of capital and the high costs of building the 5G network. The decision about the development model is, however, still being considered by the Polish government, with even the establishment of a national operator possible.[46] The attitude towards Chinese telecoms and IT companies will also have an important influence on Poland's relations with the U.S. administration, which under Trump has recently emphasised its message to partners to keep their cooperation with Huawei at arms' length, with a special emphasis on countries that already host American military bases.[47] In that regard, cooperation with Chinese enterprises may hinder Poland's goal of winning a U.S. military base. In a recent speech, the U.S. assistant secretary of state openly confirmed the importance of the evaluation of U.S. relations with its partners through the level of their cooperation with China.[48] The arrest of a Huawei executive in Poland might be considered (and already is by Chinese authorities) as Poland's participation in the U.S.'s campaign against Chinese IT enterprises. But one should remember that Poland and the U.S. share the same concerns and are justified in addressing them according to the situation. The debate on 5G, Huawei, and cooperation with Chinese IT and telecom companies is also needed on the EU level. This need was noted by EU Commission Vice President Andrus Ansip in his remarks on the security risks posed by telecom giant Huawei.[49] There is also a need for strong transparency mechanisms involving the Chinese companies and their possible involvement in critical infrastructure. In order to evaluate the factual level of the Chinese engagement, the EU will try to map the cooperation of Chinese companies with the Member States. With upcoming 5G frequency auctions in several Member States, there also is a need to coordinate on the European level efforts to prevent a single Chinese contractor from being involved in most of the winning bids. Whether the European Commission will be responsible for this coordination and how it should be organised without the use of protectionist measures or violating EU economic freedoms remains in question. There might also be a need to use certain financial initiatives (such as Germany's €1 billion fund to counter Chinese investment bids) and incentives on the EU level that might help operators in individual states should they decline a lower offer from a company such as Huawei. Differences exist in Member State policies regarding Huawei, but there is a growing sense of the need for action on the European level concerning the Chinese investments (e.g., screening mechanism) to decrease the security risks, including in the telecommunications sector. Recent discussions in the EU have steadily influenced less-positive positions in countries such as Germany and the UK on cooperation with China. Portugal[50] or Hungary remain examples of a rather positive attitude in this regard.

[46] S. Czubkowska, "Afera Huawei w Polsce nie wybuchła w przypadkowym momencie" [Huawei case not revealed by accident], *Gazeta Wyborcza*, 15 January 2019, www.gazeta.pl

[47] S. Woo, "Washington asks allies to drop Huawei," *Wall Street Journal*, 23 November 2018, www.wsj.com.

[48] It was a speech delivered on 18 October 2018 by A. Wess Mitchel, assistant secretary, Bureau of European and Eurasian Affairs. Full text at www.state.gov.

[49] F. Guarascio, Foo Yun Chee, "Europe should be wary of Huawei, EU tech official says," *Reuters,* 7 December 2018, www.reuters.com.

[50] Li Tao, "Huawei signs deal to upgrade Portugal's largest phone network Altice to 5G standards by 2019," *South China Morning Post*, 6 December 2018, www.scmp.com.

Table 1. Huawei and 5G in Selected Countries[51]

Country	Major partners and areas of cooperation	State position on cooperation with Huawei and security risks
Poland	Orange with Huawei inaugurated the first 5G trial station (in Gliwice) outside laboratories (2018). Huawei considers opening an R&D centre near Warsaw (2018). TMobile opened its first 5G lab in Warsaw with Huawei's participation (2018). A Huawei executive was detained by Poland's Internal Security Agency and a Polish court authorised arrest on the grounds of espionage (2019).	Ministry of Digitalisation in its "5G Strategy" refuses direct state engagement in the construction of 5G infrastructure. Mostly, funds from private enterprises will be used, but state support is also possible.[52] Polish authorities are considering screening state infrastructure to determine the current usage of Huawei hardware. The Government Plenipotentiary for Cybersecurity announced that a recommendation of caution using Chinese companies in the Polish IT sector may soon be issued. The minister for Internal Affairs called for a joint EU-NATO stance on the involvement of Chinese companies in IT infrastructure.
France	Bouygues Telecom and Huawei signed a 5G Joint Innovation Agreement with the first 5G network trials in Bordeaux (2018). Huawei signed a partnership with Orange to cooperate on 5G and cloud technologies (2017). Orange, however, has just reported it will not use Huawei equipment in its 5G network in the country. BG and SFR await instructions from France's National Agency for the Security of Information Systems (Anssi)	5G infrastructure to be built under private and state cooperation. The government is aware of security risks with Huawei but will not ban cooperation, though it is considering making some portion of the infrastructure inaccessible to Huawei. Huawei refused to provide its equipment to Anssi for screening (unlike Nokia, Ericsson, and Cisco).
Germany	Deutsche Telekom (DT) announced the "first 5G antennas in Europe" are now in Berlin for test operations. Huawei is the main supplier (2018). DT and Huawei achieved the first live 5G connection (2017). DT also announced it will review its network vendor strategy in light of the debate on the security of Chinese network equipment.	Government wants to continue to cooperate with Huawei on market potential but claims a need for control by the security services (BSI). BSI admits that its security lab in Bonn will give it access to Huawei source code. There is ongoing political debate in Germany on the possible limitation of Huawei's activities.[53] The decision by

[51] Table based on international press queries as well as information from www.5g-ppp.eu. Choice of countries based on the importance and exclusivity of their cooperation with Huawei.
[52] "Strategia 5G dla Polski [5G Strategy for Poland]," Ministry of Digitalisation, 5 January 2018, www.gov.pl.
[53] N. Barkin, "Exclusive: German officials raise China alarm as 5G auctions loom," *Reuters*, 13 November 2018, www.reuters.com.

	Huawei, in cooperation with the Bavarian State Government and city of Munich, launched a 5G Vertical Industry Accelerator in Munich (2015). Huawei signed an MoU with FESTO for smart-manufacturing collaboration with 5G Slicing Technology (2017). Huawei and DLR (Deutsches Zentrum fur Luft und Rumfahrt) tested 5G cooperative automated driving in Munich (2017). Huawei opened a new security lab in Bonn, Germany. It promised that it will enable source code for reviews and screening it for 'back doors' (2018).	DT is evidence of a changing attitude towards Huawei.
Russia	Beeline operator (VimpelCom PJSC) signed a two-year strategic agreement with Huawei on piloting and integrating 4.5G and 5G (May 2018). Megafon successfully tested mobile data transmission at 1 Gbps using Huawei equipment. Huawei would like to be responsible for the construction of the state's 5G network (first trials in the city of Kazan).	5G is another aspect of Russia's cooperation with China: they have already established two R&D centres (and are considering a third) and launched Huawei Pay in Russia—the first country outside China to get it. It holds a neutral position towards Huawei, and is open to cooperation.
South Korea	SK Telecom chose Ericsson and Nokia instead of Huawei as vendors to build its 5G network (2018). Huawei may still keep its work with LG U+ (they already have cooperation on 4G). SK Telecom, KT Corp., and LG U+ signed initial 5G contracts with Huawei (2018).	No official ban but unconfirmed news about pressure on operators to not choose Huawei as their equipment partner in 5G infrastructure.
Czech Republic	Vodafone started a 5G test in Karlove Vary with Huawei. The 5G mobile internet speed reached 1.84 Gbps.	In an agreement signed by Czech President Miloš Zeman, Huawei and Czechinvest representatives projected the investment in the Czech Republic of more than $8 billion. Huawei has supplied the government and presidential office with its equipment. (2017). The National Bureau for Cyber and Information Security announced that several companies and institutions need to secure their equipment from Chinese entities. Prime Minister Andrej Babiš ordered government institutions to remove Huawei equipment. There is also a plan to get rid of Huawei equipment from the public sector in 10 years (announced in 2018). Due to internal political disputes, the Czech president has criticised the security

		agencies over their warnings about Huawei.
Hungary	Magyar Telekom (a DT company) presented its first 5G connection in cooperation with Huawei and using its equipment (2018).	Minister on Innovation and Technology in Hungary signed an MoU with Huawei on building 5G infrastructure (2018).
United States	US security regulations target Chinese telecoms (e.g., no government institutions are allowed to buy equipment from Huawei). The U.S. tariffs (25% on Chinese electronics) has, e.g., stopped the launch of Huawei's new solar panel electronic devices project.	The National Security Council recommends building nationwide, centralised, and state-controlled 5G infrastructure. The state will regulate the 5G infrastructure, with an estimated worth of $411 billion. The State Department issued an informal notice of concern to its foreign partners on Huawei's activities and its anxiety over possible involvement in 5G infrastructure.
UK	British Telecom (via the EE mobile arm) launched a 5G test network with Huawei equipment (November 2017). EE and Huawei together established a 4G network in the UK, but BT recently announced it will strip Huawei equipment from its 4G network. BT extended a strategic partnership with Huawei on 5G cooperation (2018). According to BT (owner of EE) Huawei was excluded from bidding to provide 5G equipment but will use its kits in parts of the network. Vodafone and Huawei carried out 5G tests (2016). Three (Hutchison) chose Huawei as its partner for a 5G network (unlike 3G, with Nokia, and 4G, with Samsung)	Huawei is a concern for the UK, the conclusion after a review of UK telecoms; the 5G supply chain may be affected. Specifics include considerations in procurement decisions, a letter to telecoms by the head of the National Cyber Security Centre, and MI6 warnings on the use of Huawei equipment.
Canada	Bell Telecom conducted 5G trials with Huawei in the Ontario region on wireless-to-home infrastructure (2018). Telus and Huawei launched a 5G wireless-to-home trial service in Vancouver (February 2018).	PM Trudeau refused to let "politics slip into" the decision to allow Huawei into 5G in Canada. The Canadian Security Intelligence Service told MPs that Canada has a system to identify possible security breaches. Huawei already is not allowed to bid on telecoms and is blocked from government contracts. Canada is doing a security review of 5G and has made no decision on restrictions on Huawei in this area.
Australia	Because of a government ban, Telstra, Optus, and Vodafone will have to change Huawei as their vendor for 5G equipment because it was	Use of Huawei and ZTE devices in 5G critical infrastructure is not allowed for security reasons. There is an official

	also their vendor for 4G equipment. That will raise the cost and delay implementation.	government ban on Huawei and ZTE in state tenders for 5G infrastructure (based on unconfirmed pressure from the U.S.).
India	Huawei started talks for 5G trials with operators. Conducted a 5G lab trial with Bharti Airtel (2018).	In October 2018, India's Department of Telecommunications approved Huawei (but not ZTE) as a vendor to conduct trials of 5G infrastructure in, e.g., New Delhi. Nokia, Samsung, Ericsson, and Cisco were also invited.
Italy	Telecom Italia and Fastweb launched the first country 5G base station in the city of Bari and put it into commercial use (2018). Telecom Italia signed a partnership with Huawei to provide advanced net solutions to businesses in Italy (2018). Vodafone Italia completed the first 5G data connection in Italy using Huawei and Nokia networks and devices in Milan (2018)	No direct opposition towards Huawei and 5G. The government holds "Golden Power" over Telecom Italia, which allows it to take actions to protect the strategic interests of the country.
New Zealand	The operator Spark announced its first live 5G mobile tests in Wellington with Huawei equipment (March 2018).	GCSB (Government Communications Security Bureau) banned Spark from using Huawei equipment. The TICSA act allows technology used by operators to be vetted by the bureau. (November 2018)