

RED WATCH REPORT

HUAWEI'S GEOSTRATEGIC ROLE



EUROPEAN VALUES

Protecting Freedom

2020

EUROPEAN VALUES CENTER FOR SECURITY POLICY

European Values Center for Security Policy is a non-governmental, non-partisan institute defending freedom and sovereignty. We protect liberal democracy, the rule of law, and the transatlantic alliance of the Czech Republic. We help defend Europe especially from the malign influences of Russia, China, and Islamic extremists.

We envision a free, safe, and prosperous Czechia within a vibrant Central Europe that is an integral part of the transatlantic community and is based on a firm alliance with the USA.

Author

Charles Burton, Senior Fellow, Macdonald-Laurier Institute & European Values Center for Security Policy

With support of



Notice

This is a joint publication of Konrad-Adenauer-Stiftung and the European Values Center for Security Policy. Konrad-Adenauer-Stiftung assume no responsibility for facts or opinions expressed in this publication or any subsequent use of the information contained therein. Sole responsibility lies on the author of the publication.

Image Copyright:

Page 6: flickr.com/thierry ehrmann

Page 14: flickr.com/U.S. Department of State

CONTENTS

SUMMARY	3
INTRODUCTION	5
1. HUAWEI'S CORPORATE STRUCTURE AND RELATIONSHIP TO THE PRC STATE, MILITARY AND SECURITY APPARATUS	7
2. HUAWEI'S COLLABORATION IN CHINESE STATE SURVEILLANCE AND ESPIONAGE	10
3. HUAWEI'S ROLE IN THE BRI AND XI JINPING'S "COMMUNITY OF THE COMMON DESTINY OF MANKIND"	14
4. THE PRC'S HUAWEI STRATEGY TO DOMINATE GLOBAL TELECOMMUNICATIONS	16
5. WHAT WE KNOW ABOUT U.S. INTELLIGENCE ON HUAWEI'S 5G CHALLENGE TO DOMESTIC AND GLOBAL SECURITY	20
6. U.S. MEASURES TO CONTAIN HUAWEI AND THE PRC'S COUNTERMEASURES	22
CONCLUSION: THE FUTURE OF HUAWEI 5G IN CHINA'S GEOSTRATEGY AND THE WEST'S RESPONSE	23
APPENDIX: NATO STATES RESPONSE TO 5G & HUAWEI (COMPILED BY THE EUROPEAN VALUES CENTER FOR SECURITY POLICY)	25

SUMMARY

- Huawei is mobilized by the Chinese Communist's Party to serve PRC regime geostrategic goals throughout the world under the rubric of "the community of the common destiny of mankind.
- Because of its role as an integral element of the unified Communist Party regime Huawei's primary purpose is not to generate profits, but to serve the overall interests of the Chinese Communist Party at home and abroad.
- Huawei can reciprocally draw on PRC Party-State military and intelligence services to obtain technology and data to its competitive advantage.
- It is fully supported by the Chinese Communist Party's extensive United Front Work Department operations coordinated out of the PRC's embassies and consulates abroad.
- Huawei is complicit in the massive surveillance program against the Uyghurs and other Turkic Muslim peoples living in China's northwestern territory; Huawei plays a key role in developing the CCP's dystopian social credit program; Huawei is complicit in China's great firewall and internet censorship that violates freedom of expression; Huawei exports China's technologies of censorship and extreme surveillance to dictatorships throughout the world as part of its Digital Silk Road program; There is pervasive use of Huawei technologies for cyber-espionage; Huawei has been charged with fraud, obstruction of justice, and theft of trade secrets.
- Huawei's corporate behavior has been morally egregious because it is complicit in enabling the use of digital technologies in ways that are so counter to Western liberal values making it an unethical partner for Western nations to do business with, as is the case with PRC Party-State associated firms
- Gaining support for permitting Huawei to install 5G into national telecommunications systems is so critical to the PRC regime of which Huawei is a part. This is because it has the potential to facilitate massive transfer of data to China that through analysis by sophisticated artificial intelligence algorithms which would allow identification of potential targets for espionage and United Front Work.
- Ultimately Huawei could facilitate PRC knowledge of critical digital infrastructure including key resources such as water, electricity, internet service, etc. The capacity to install kill switches into Huawei digital pipelines would provide China with key advantage.
- The offering of Huawei technology to China-friendly dictatorial rulers to allow them to sustain their political power by surveillance against potential dissidents and restricting the flow of information to an oppressed people renders them amenable and beholden to China's authoritarian Chinese Communist Party regime.
- There are multiple Chinese state subsidies to Huawei: hundreds of millions of dollars in grants, heavily subsidized land for facilities, buildings and employee apartments, and massive state loans and Chinese state banks providing favourable loan terms to 3rd world nations buying Huawei installations.
- Chinese Party-State puts considerable resources put into engaging persons of political influence such as former politicians and senior political staffers to lobby governments to accept Huawei 5G.
- The U.S. is concerned about "the potential loss of control over U.S. 'critical infrastructure'; the interdependent system of electric power grids; banking and finance systems; natural gas, oil, and water systems; and rail and shipping channels – each of which depend on computerized control systems."
- The U.S. House Permanent Select Committee on Intelligence has further concerns over Chinese motivations and their capacity to maliciously modify or steal information from government and

corporate entities in order to gain access to expensive and time-consuming research and development that would advance China's economic position on the world stage.

- The U.S. has also made it clear to its Five Eyes Intelligence Alliance that the U.S. cannot entrust secret information to any partner that allows Huawei 5G into its national telecommunications network.
- In September 2020, the United States enacted a ban that prohibits any company from selling semi-conductors to Huawei that rely on U.S. hardware or design software. So Japanese firms such as Sony, Kioxia and Renesas, which had supplied an estimated US\$14.4-billion in parts to Huawei in 2019 stopped shipments in mid-September 2020. Unless some resolution is made, Huawei could be short of critical components to manufacture handsets and 5G network hardware by early in 2021.
- The U.S. has taken action to deny Huawei access to Google Android Apps. Because Huawei cannot manufacture its equipment using Chinese chips, nor can it duplicate the variety quantity and quality of Android apps available through Google, these measures are crippling to Huawei's global competitiveness.
- The critical imperative to gain control of global telecommunications to exert more influence is deeply embedded in the legitimating mission of the Chinese Communist Party. If it is not Huawei, one could expect that one day in the future, when PRC has retrenched to self-sufficiency in production of the hardware and software necessary to dominate over all international competitors in telecommunications networks throughout the world, that possibly under a different corporate name, the regime will reapply its ambition to dominance and control over global telecommunications to further strive to realize its dream of the of the great rejuvenation of the Chinese nation.

INTRODUCTION

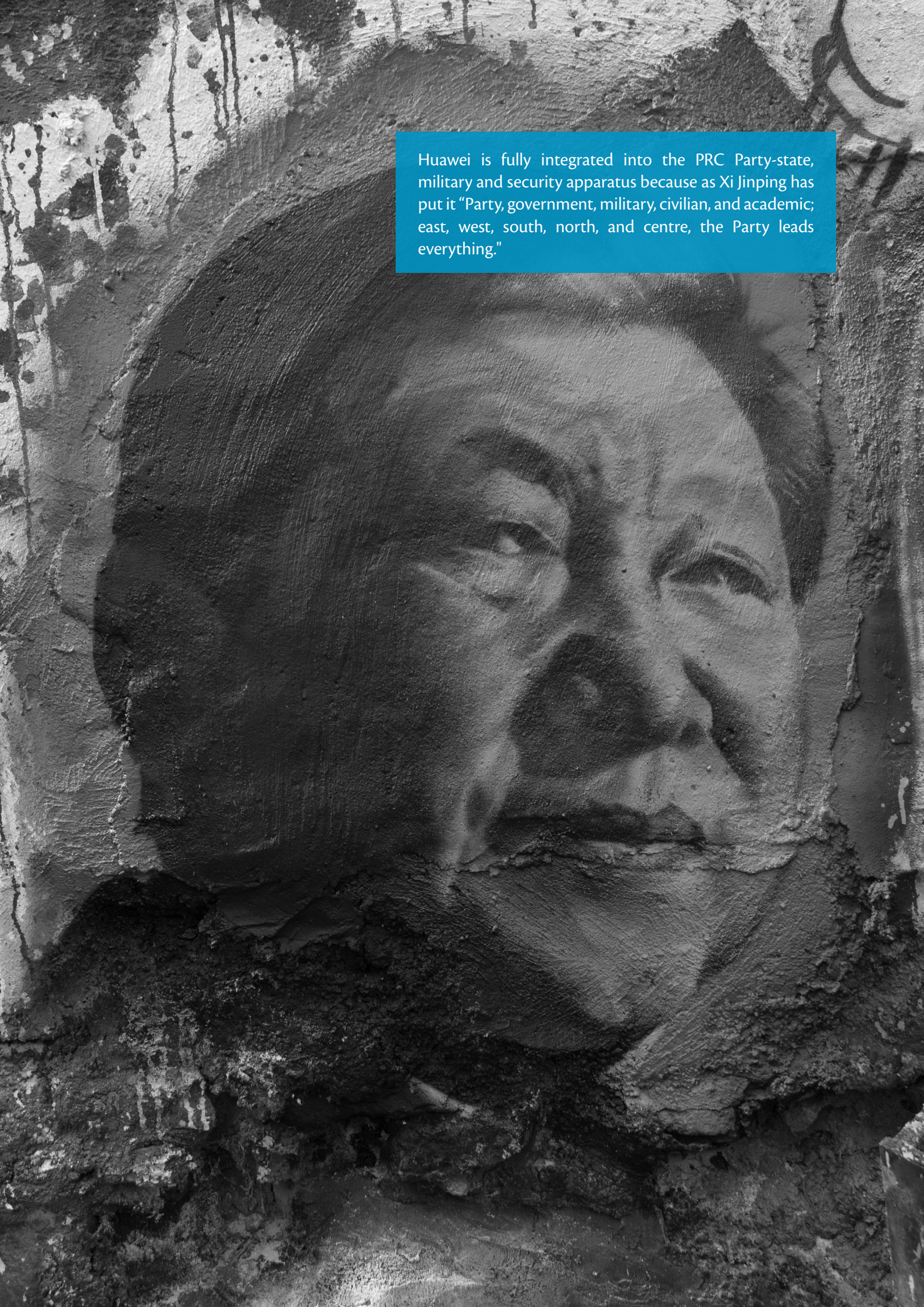
The geostrategic implications of Huawei's bid to dominate global 5G telecommunications networks pose an enormous challenge to the West. But the nature and gravity of this challenge is still inadequately appreciated by people outside of China. The symbiotic relationship of Huawei to China's integrated Party-state-military regime is difficult for people in the free world to comprehend. The PRC's sophisticated and comprehensive influence operations put considerable resources into downplaying Huawei's role in China's hegemonistic global agenda. Huawei's public relations narrative is that Huawei is an exceptionally well-managed exemplary corporate citizen that is the victim of the U.S.'s foreign policy agenda to suppress China's rightful and peaceful rise to power.

But the allegations that Huawei technology is complicit in espionage, massive surveillance in China and abroad enabling gross violations of human rights by the PRC regime, and instrumental in the transferring of huge foreign databases to the PRC, done more and more blatantly as China's global confidence rises, are increasingly well documented.

More significantly, Huawei technology is a critical element in China's mobilization to develop what Xi Jinping has characterized as "the community of the common destiny of mankind," a reorientation of all global multilateral institutions in diplomacy and trade to a China-centric world order supported by Beijing's Belt and Road Initiative which will restructure global infrastructure to put China at the centre of international trade and investment and strategic relations. A crucial goal to support this overall scheme is to engender the conditions to have Huawei 5G technology dominate all global communications to serve the needs of Chinese cyber-espionage and facilitate Chinese military advantage over infrastructure in all critical areas everywhere on the planet. The Chinese state heavily subsidizes Huawei hardware and software development and production to make it highly competitive in global markets.

But over the past three years, the Government of the United States has become increasingly aware of the security threat that Huawei technology poses to the U.S. and to the world. It has engaged in a series of measures to prevent Huawei from becoming the dominant force in global communications. These include enacting measures to prevent chip makers from supplying Huawei and threatening to cease sharing military and diplomatic intelligence with Western nations that allow Huawei 5G kit to be installed in their national telecommunications networks.

All the above calls for Western nations to advance policies and legislation to ensure that engagement with the PRC at all levels is of benefit, and not damaging, to their national interest and of benefit to the maintenance of the integrity of the norms of fairness and reciprocity that underlie the rules-based international order.



Huawei is fully integrated into the PRC Party-state, military and security apparatus because as Xi Jinping has put it "Party, government, military, civilian, and academic; east, west, south, north, and centre, the Party leads everything."

1. HUAWEI'S CORPORATE STRUCTURE AND RELATIONSHIP TO THE PRC STATE, MILITARY AND SECURITY APPARATUS

Huawei's public relations, directed to the Western audience, depict Huawei as simply a successful privately held multinational company, a counterpart and competitor to other major telecommunications concerns such as Ericsson, Nokia, or Samsung. The assertion is that, like them, Huawei's primary corporate purpose is to maximize profit for its shareholders. Huawei claims it is in fact owned by its employees which gives incentive for these employee/shareholders to work efficiently and in harmony with each other to the economic and social benefit of all.¹

The explanation for Huawei's ability to undercut its competitors and win contracts to install its 3G and 4G technology into more networks throughout the world than any of its competitors is attributed to its hard-charging "wolf culture." Huawei maintains that its corporate "wolf culture" demands that its employees work harder and with more intensity of purpose than the employees of other companies in other nations. "The first character of wolves is bloodthirsty. Employees of Huawei are extremely sensitive to the market information and could response promptly to any changes. The second character of wolves is resistant to coldness. The fearlessness of difficulties and eagerness of making progress are insisted by every member of Huawei, no matter how complicated the hardship is. The third character of wolves is taking actions in teams. The atmosphere of team cooperation is particularly strong in Huawei and people are encouraged to develop and share personal opinions with each other... it's no doubt that the 'wolf-culture' is the cornerstone of success for Huawei and lead Huawei to make significant breakthroughs in such competitive market of modern society."² [sic]

Huawei has committed to aggressively adapting to conditions in Third World countries to get ahead in those markets. For example, in desert nations bedeviled by massive infiltrations of wire-gnawing rats, unlike its competitors, Huawei realized it had to put in thicker cables to do business. "The multinational telecom companies providing service at that time did not consider this to be their problem, but rather that of the customer. Huawei, in contrast, viewed the rat problem as one the company had the responsibility to solve. In doing so, they acquired extensive experience in developing sturdier equipment and materials — such as chew-proof wires — which helped them later on to gain several big business accounts in the Middle East, where similar problems stymied the multinational firms."³

And we are told that Huawei's engineers excel at technical innovation, which is why Huawei offers a superior product at a cheaper price and wins major contracts to install national telecommunications systems. Granted, some of Huawei's methods to gain strategic advantage over the competition may have been beyond the pale. The revelations of an employee incentive scheme for employees who steal competitors' hardware and software are one sign.⁴

Another major factor is the key role of Ren Zhengfei, Huawei's founder and CEO. His is a rags-to-riches story.⁵

1 This is a highly dubious claim. See Zhong, Raymond. "Who Owns Huawei? The Company Tried to Explain. It Got Complicated." The New York Times, April 26, 2019, sec. Technology. <https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html> and Balding, Christopher and Clarke, Donald C., Who Owns Huawei? (April 17, 2019). Available at SSRN: <https://ssrn.com/abstract=3372669>.

2 Huawei Australia. "Our Culture." Huawei: For a Better Connected World (blog), May 8, 2014. <https://huaweico.wordpress.com/our-culture/>.

3 De Cremer, David, and Tian Tao. "Huawei's Culture Is the Key to Its Success." Harvard Business Review, June 11, 2015. <https://hbr.org/2015/06/huaweis-culture-is-the-key-to-its-success>.

4 Bastone, Nick. "Chinese Electronics Giant Huawei Allegedly Offered Bonuses to Any Employee Who Stole Trade Secrets." Business Insider. Accessed September 23, 2020. <https://www.businessinsider.com/huawei-indictment-trade-secrets-2019-1>.

5 Ren Zhengfei is said to have started Huawei in 1987 with less than 4,000 Euros capital. Huawei EU. "A Truly Global Culture." Huawei, May 6, 2020. <https://huawei.eu/story/truly-global-culture>.

Ren is much lauded as having dedicated his life, body, and soul to the furtherance of Huawei's global rise as China's greatest success story in the international market. His motive and reward are deep pride in bringing glory to the Chinese nation in this way. After all, Mr. Ren is a former military man and a member of the Chinese Communist Party (the People's Liberation Army is sworn to be loyal to the Party alone and not to the Chinese state). Nevertheless, despite China's National Security Law demanding that all Chinese citizens collaborate with intelligence agencies on demand, Mr. Ren has emphatically insisted that Huawei would never endanger its competitive position by engaging in activities against the law in those countries where Huawei has operations. As an article lauding Huawei's success puts it, "Strong leaders provide a sense of purpose to their people, and Ren Zhengfei is no exception. His first and foremost concern is the customer. Many companies adopt a customer-focused attitude, but how many of them truly live it? Huawei distinguishes itself from the competition in this regard."⁶ [sic]

The above is a discourse that Western nations' telecommunications companies whose mandate is to provide cell 'phone and data services service at the best rate to as many customers as possible, and who have no corporate mandate to defend their nation's national security against PRC operations, would prefer is true (and having to switch out their 3G and 4G Huawei installations to be compatible with non-Huawei 5G will be very costly).⁷ But this PR discourse is manifestly false. Indeed, accepting the blithe claim that Huawei's *raison d'être* is primarily economic profitability, and that Huawei simply brings honour to China as a multinational corporate success story, dangerously engenders a false sense of security among its foreign national targets.⁸

The language of China's National Intelligence Law seen as compelling all Chinese nationals working for Huawei to collaborate with agents of the Chinese state on request to further Chinese state interests by purloining confidential data and engaging in compromise of infrastructure around the world is a *pro forma*.⁹ While Huawei CFO, Ren Zhengfei claims Huawei would never comply with an PRC regime request to hand over customer's data.¹⁰ In fact, Huawei's connection to the Chinese Party-Military state is much more than a servant-master relationship. It is indeed a symbiotic relationship. Huawei is fully integrated into the PRC Party-state, military and security apparatus because as Xi Jinping has put it "Party, government, military, civilian, and academic; east, west, south, north, and centre, the Party leads everything."¹¹ Just as China does not allow true civil society as a non-government sector,¹² there are no PRC-based industrial enterprises existing independently from China's Party-State.¹³ While Huawei is not deemed a state-owned enterprise as such, it is still an integral component of China's Communist Party regime.

The Huawei corporate organigram shows its Chinese Communist Party branch and its Party Secretary Zhou

6 Huawei EU. "A Truly Global Culture." Huawei, May 6, 2020. <https://huawei.eu/story/truly-global-culture>.

7 Karam, Amy. "Why Bell, Telus Want to Pick Huawei for 5G Networks, despite Debate over Security Concerns." The Hill Times (blog), June 8, 2020. <https://www.hilltimes.com/2020/06/08/why-bell-telus-want-to-pick-huawei-for-5g-networks-despite-debate-over-security-concerns/251804>.

8 See for example RWR Advisory Group. "Huawei Risk Tracker." RWR Advisory Group. Accessed September 21, 2020. <https://huawei.rwradvisory.com/>.

9 Canadian Security Intelligence Service. "China's Intelligence Law and the Country's Future Intelligence Competitions." aem, May 10, 2018. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html>.

10 Kharpal, Arjun. "Huawei CEO: No Matter My Communist Party Ties, I'll 'definitely' Refuse If Beijing Wants Our Customers' Data." CNBC, January 15, 2019. <https://www.cnbc.com/2019/01/15/huawei-ceo-we-would-refuse-a-chinese-government-request-for-user-data.html>.

11 Merics China Monitor. "The Party Leads on Everything." Merics, September 24, 2019. <https://merics.org/en/report/party-leads-everything>.

12 Haas, Benjamin. "China 'eliminating Civil Society' by Targeting Human Rights Activists – Report." the Guardian, February 16, 2017. <http://www.theguardian.com/world/2017/feb/16/china-eliminating-civil-society-by-targeting-human-rights-activists-report>.

13 McGregor, Richard. "How the State Runs Business in China." The Guardian, July 25, 2019, sec. World news. <https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei>.

Daiqi at the apex of Huawei's corporate pyramid.¹⁴ This has been dismissed by Huawei's foreign apologists as a formality with no substantive meaning (of course no one in China would dare say that).¹⁵ But a parallel can be drawn between the PRC's constitutional fiction that the rubber stamp National People's Congress is the "supreme organ of state power",¹⁶ whereas ultimate and unassailable political power in China in fact rests with the Standing Committee of the Political Bureau of the Central Committee of the Communist Party. Huawei is of an utterly different substantive nature than its foreign competitors who exist in the civil space outside of liberal democratic political institutions. It is a hugely significant distinction between Huawei and non-Chinese telecommunication concerns. Huawei's purposes are actually the Chinese Communist Party's purposes for Huawei.¹⁷

But the PRC keeps this strictly hidden. As early as 2012, the U.S. House Intelligence Committee following an investigation of Huawei and ZTE released a report showing "The Committee received almost no information on the role of Chinese Communist Party Committee within Huawei or specifics about how Huawei interacts in formal channels with the Chinese government," the report said. "Huawei refused to provide details about its business operations in the United States, failed to disclose details of its dealings with the Chinese military or intelligence services and would not provide clear answers on the firm's decision-making processes."¹⁸ A recent British parliamentary report affirms the strong collusion between Huawei and the Chinese Communist Party.¹⁹ It is fully supported by the Chinese Communist Party's extensive United Front Work Department operations coordinated out of the PRC's embassies and consulates abroad.²⁰

14 Huawei. "Mr. Zhou Daiqi - Huawei Executives." Huawei Technologies. Accessed September 21, 2020. <https://www.huawei.com/en/executives/supervisory-board/zhou-daiqi>. The organigram showing the Party leadership at the top was previously publicly available but has evidently since been scrubbed from the internet "Reportedly, as of 2007, Huawei's party committee managed 56 general branches (总支), controlled 300 party branches (党支部) and had over 12,000 members... Huawei's current Party Secretary is Zhou Daiqi (周代琪), who has served simultaneously as Chief Ethics & Compliance Officer and Director of the Corporate Committee of Ethics and Compliance. However, Zhou Daiqi often seems to represent Huawei in his official capacity as Party Secretary (党委书记) and senior vice president) for high-level talks and occasions, such as the signing of a strategic cooperation agreement with a municipal government on the creation of a cloud computing data centre": Kania, Elsa. "Much Ado about Huawei (Part 2)." The Strategist, March 28, 2018. <https://www.aspistrategist.org.au/much-ado-huawei-part-2/>.

15 "Our founder Ren Zhengfei is a member of the CPC but this has no bearing on the business. To explain why, it is useful to put this into its historical context. When Ren Zhengfei was a young man, you needed to be a CPC member to have any position of responsibility, even as the head of a cooking team in the military." Huawei Facts. "Does Huawei Have Ties to the Communist Party of China (CPC)?" Huawei Technologies. Accessed September 21, 2020. <https://www.huawei.com/en/facts/question-answer/does-huawei-have-ties-to-the-cpc>.

16 Global Times. "NPC: Supreme Organ of State Power in China." Global Times, March 8, 2011. <https://www.globaltimes.cn/content/631036.shtml>.

17 McGregor, Richard. The Party: The Secret World of China's Communist Rulers. New York, NY: Harper, 2010.

18 Fazzini, Kate. "Why the US Government Is so Suspicious of Huawei." CNBC, December 6, 2018. <https://www.cnbc.com/2018/12/06/huaweis-difficult-history-with-us-government.html>.

19 Corera, Gordon. "Huawei: MPs Claim 'clear Evidence of Collusion' with Chinese Communist Party." BBC News, October 7, 2020, sec. Technology. <https://www.bbc.com/news/technology-54455112>.

20 Brady, Anne-Marie. "Magic Weapons: China's Political Influence Activities under Xi Jinping." Wilson Center, September 18, 2017. <https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influence-activities-under-xi-jinping>.

2. HUAWEI'S COLLABORATION IN CHINESE STATE SURVEILLANCE AND ESPIONAGE

Huawei Europe avers that: "Everywhere Huawei operates, it abides by the local laws. Huawei also observes the conventions of the United Nations."²¹ This is certainly a powerful statement of commitment to high principles of corporate social responsibility. Promising to uphold the conventions of the UN in its operations certainly goes beyond the scope of ethics and morality undertaken by most Western nation profit driven business entities.

One is struck by how this fits with Huawei's complicity in the massive surveillance program against the Uyghurs and other Turkic Muslim peoples living in China's northwestern territory. Huawei installations provide the software and hardware surveillance means by which the Chinese Communist Party identifies those Uyghurs who meet the criteria for arrest and relocation to cultural genocide concentration camps in huge numbers.²² It is the backbone of the facial recognition technology to see who goes where and who meets with whom. Huawei enables the artificial intelligence to analyze conversations in the Uyghur language picked up by hidden microphones or relayed by telephone or social media.²³ British Uyghur Rahma Makmut, who heads the London office of the World Uyghur Congress, wrote a public letter to the Government of the United Kingdom in October 2020 urging non-adoption of Huawei 5G on that basis that "[s]ince 2016, my homeland has been turned into the biggest digital gulag on earth, and Huawei has been working with the public security bureau, providing surveillance technology which is being used to arbitrarily detain millions of my people. It's a disgrace that a company that is central to the oppression and suppression of an entire ethnic population has been given such an important role within the infrastructure of the United Kingdom. It is a betrayal of the core values and morals that I believed this country stood for as a British citizen. The entire Uyghur population both inside the Uyghur region and in exile are suffering from the CCP's oppressive surveillance technology."²⁴ Proof of Huawei's direct involvement and support of surveillance and intelligence gathering technology used to suppress the human rights of Uyghurs has been compiled by the Australian Strategic Policy Institute in its in depth study, "Uyghurs for Sale: 'Re-education,' Forced Labour and Surveillance Beyond Xinjiang".²⁵

And what of Huawei's role in developing the dystopian social credit program that demands that all Chinese people have all their comings and goings, with whom they associate, their purchases, what they read, what they write, their internet usage, and with whom they associate? Before long, even what they say in public and in private will be assessed according to the repressive criteria of China's authoritarian one-party regime by sophisticated algorithms analyzing massive databases links. This is well beyond anything that George Orwell could have conceived as he was writing his novel, 1984.²⁶

And what of Huawei's complicity in China's great firewall and internet censorship that violates freedom of

21 Huawei EU. "A Truly Global Culture." Huawei, May 6, 2020. <https://huawei.eu/story/truly-global-culture>.

22 Ingram, Ruth. "Huawei, 5G and Human Rights Abuses: Yes, They Are Connected." Association for the Defense of Human Rights and Religious Freedom, May 2, 2020. <https://en.adhrrf.org/Huawei-5G-and-Human-Rights-Abuses-Yes-They-Are-Connected.html>.

23 Vanderklippe, Nathan. "Huawei Providing Surveillance Tech to China's Xinjiang Authorities, Report Finds." Globe and Mail, November 29, 2019. <https://www.theglobeandmail.com/world/article-huawei-providing-surveillance-tech-to-chinas-xinjiang-authorities/>.

24 Ingram, Ruth. "Huawei, 5G and Human Rights Abuses: Yes, They Are Connected." Association for the Defense of Human Rights and Religious Freedom, May 2, 2020. <https://en.adhrrf.org/Huawei-5G-and-Human-Rights-Abuses-Yes-They-Are-Connected.html>.

25 Ruser, Vicky Xiuzhong Xu, Danielle Cave, James Leibold, Kelsey Munro, Nathan. "Uyghurs for Sale." Australian Strategic Policy Institute International Cyber Policy Centre, March 1, 2020. <https://www.aspi.org.au/report/uyghurs-sale>.

26 Blumenthal, Dan. "Huawei Is the Doorway to China's Police State." Text. The National Interest. The Center for the National Interest, December 12, 2018. <https://nationalinterest.org/feature/huawei-doorway-chinas-police-state-38532>.

expression?²⁷ And what of the export of China's technologies of censorship and extreme surveillance China offers to dictatorships throughout the world as part of its Digital Silk Road program? Does it in effect enable the grip of authoritarian repression in nations throughout the globe struggling to achieve strengthening of their democracy and citizens' entitlement to fundamental human rights.²⁸

And then there has been the pervasive use of Huawei technologies for cyber-espionage. These allow the Chinese regime to engage in influence operations, and the acquisition of technologies the further facilitate repression and allow China's regime to enhance its military threat and fulfill its geostrategic ambitions. In 2015, China stole the personnel records of over 4 million U.S. government personnel.²⁹ China without question does much more cyber-espionage than any other nation by far.³⁰

Two former managers at the multinational's Czech unit told Czech public radio in 2019 that they were required to enter people's personal details into an internal database. This included details like number of children, personal interests, and financial situation. They further claimed that they had to gather information on state officials, mainly department directors or deputy ministers, who would then be invited to conferences in China. According to the report it was also standard practice for Huawei employees to share the information they gathered at meetings with Chinese embassy officials.³¹

Huawei is using a wide range of methods and techniques — everything from cyber intrusions to corrupting trusted insiders. They've even engaged in physical theft. And they've pioneered an expansive approach to stealing innovation through a wide range of actors — including not just Chinese intelligence services, but also state-owned enterprises, ostensibly private companies, in universities and research institutes deploying graduate students and researchers, and a variety of other actors all working on their behalf.³²

Inside China, foreign enterprises operate in a highly compromised environment. As Christopher Wray, Director of the U.S. Federal Bureau of Investigation, puts it: "They should also think about what it means to operate in an environment where a major IT provider like Huawei, with broad access into so much that U.S. companies do in China, has been charged with fraud, obstruction of justice, and theft of trade secrets. There's no reason for any U.S. company working in China to think it's safely off-limits."³³

The issue is fundamentally one of trust. And this distrust extends to any enterprise under the aegis of the Chinese Communist Party. In 2017, Le Monde reported that confidential data on the IT network of the Chinese-built African Union headquarters in Ethiopia was being siphoned off to Shanghai every night between 2012 and 2017. Similarly, the Canadian Department of National Defence was forced into considerably moving its new headquarters at a former Nortel Networks complex because the building was riddled with Chinese

27 Herman, Arthur. "Huawei's (And China's) Dangerous High-Tech Game." Forbes.com, December 10, 2018. <https://www.forbes.com/sites/arthurherman/2018/12/10/huaweis-and-chinas-dangerous-high-tech-game/#f2db0b211ab7>.

28 Triolo, Robert, and Paul Greene. "Will China Control the Global Internet Via Its Digital Silk Road?" Carnegie Endowment for International Peace, May 8, 2020. <https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857>.

29 Nakashima, Ellen. "Chinese Breach Data of 4 Million Federal Workers." Washington Post, June 4, 2015, sec. National Security. https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

30 Sanger, David E., David Barboza, and Nicole Perlroth. "China's Army Is Seen as Tied to Hacking Against U.S." New York Times, February 18, 2013. <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>.

31 Kroupa, Janek. "Počet dětí, zájmy, majetek. Český Huawei podle exmanažerů řeší klienty s lidmi z čínské ambasády." iROZHLAS, July 22, 2019. https://www.irozhlas.cz/zpravy-domov/kauza-huawei-cina-spionaz-citlive-udaje-klientu-cesty-do-zahranici-gdpr_1907220600_per.

32 Armstrong, Peter, "Huawei Funds \$56M in Academic Research in Canada. That Has Some Experts Concerned | CBC News." CBC, November 29, 2019. <https://www.cbc.ca/news/business/huawei-academic-funding-in-canada-1.5372310>.

33 Wray, Christopher. "Responding Effectively to the Chinese Economic Espionage Threat." Speech. Federal Bureau of Investigation, February 6, 2020. <https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat>.

eavesdropping devices.³⁴ China's pervasive flouting of the norms of international trade and diplomacy by use of trade sanctions in violation of its commitment to the WTO to express its displeasure over such mundane matters as the Australian Government's call to properly investigate the sources and early transmission of COVID-19³⁵ or the use of "hostage diplomacy" to pressure western nations on political matters³⁶ has rightly led to international public opinion turning sharply against the Chinese regime.³⁷

In assessing the adoption of Huawei equipment into a nation's telecommunications backbone, there's also a moral factor. Do nations of the world wish to transfer resources to purchase software and hardware solutions from a company whose corporate behavior has been morally egregious, that is complicit in enabling the use of digital technologies in ways that are so counter to Western liberal values and indeed the liberal principles that inform the United Nations conventions that Huawei speciously claims to uphold?

34 CTC News.ca Staff. "DND May Abandon \$1B Move to Former Nortel Site Because of Surveillance Bugs." CTVNews, September 30, 2013. <https://www.ctvnews.ca/canada/dnd-may-abandon-1b-move-to-former-nortel-site-because-of-surveillance-bugs-1.1477766>.

35 Westcott, Ben. "Australia Barley Exports: Beijing Targets Canberra after Calls for a Coronavirus Investigation - CNN." CNN Business, May 27, 2020. <https://www.cnn.com/2020/05/26/business/china-australia-coronavirus-trade-war-intl-hnk/index.html>.

36 Thomson, Stuart. "China Steps up Use of 'hostage Diplomacy' in International Relations: Experts." National Post, August 31, 2020. <https://nationalpost.com/news/politics/china-steps-up-use-of-hostage-diplomacy-in-international-relations-experts>.

37 Buckley, Chris. "Distrust of China Jumps to New Highs in Democratic Nations - The New York Times." New York Times, October 6, 2020. <https://www.nytimes.com/2020/10/06/world/asia/china-negative-pew-survey.html>.



Xi Jinping is confident that the United States is in rapid decline as a global power. China will inevitably rise to fill the vacuum caused by the fall of the U.S. as the global superpower.

3. HUAWEI'S ROLE IN THE BRI AND XI JINPING'S "COMMUNITY OF THE COMMON DESTINY OF MANKIND"

Communist Party General Secretary Xi Jinping assumed supreme power over China in November 2012. His predecessors, Jiang Zemin and Hu Jintao, rested their political legitimacy on promoting China's prosperity by a continuous process of "opening up to the outside world," modernization, political reform and "getting on track" with norms of global institutions. They promised all this "under the leadership of the Chinese Communist Party" upholding "socialism with Chinese characteristics."³⁸

"Xi Jinping has made a radical split from this discourse. Under his predecessors, the Party had become more and more out of sync with prevailing modern social values in the PRC and perceived as increasingly irrelevant and corrupt. Xi has sought to revitalize the Party by reaffirming the Stalinist institutions that structure its power, reinforcing Leninist norms as the basis for a massive and effective anti-corruption campaign, and reinvigorating the Party as the locus of the greatness of China's civilizational tradition in the contemporary era.³⁹ He has attempted to reinspire popular enthusiasm for Chinese Communist Party rule by promising "to achieve the Chinese dream of the great rejuvenation of the Chinese nation."⁴⁰

The plan is that by the 100th anniversary of the establishment of the People's Republic of China, that is in the year 2050, China will be a "strong, democratic, civilized, harmonious, and modern socialist country."⁴¹

But there is more in terms of China's future international role. Xi Jinping has proposed a China-led global international order he dubs "the community of the common destiny of mankind." The existing multilateral institutions of the post-War U.S.-led rules-based order are derived from liberal values that Xi has denounced as incompatible and hostile to China's geostrategic ambitions. Xi Jinping is confident that the United States is in rapid decline as a global power. China will inevitably rise to fill the vacuum caused by the fall of the U.S. as the global superpower. The U.N. and WTO will fade into irrelevance and new China-inspired and led institutions will come to the fore. This is "the community of the common destiny of mankind."⁴²

In terms of global economics, the Belt and Road Initiative (BRI) is a Chinese global infrastructure program designed to reorient the global economy around China, for which the two characters in the country's Chinese language name, zhong and guo literally mean "the Middle Kingdom." The BRI's Belt is roads and rail links connecting all of Eurasian from China to Spain. The BRI's Road is the Maritime Silk Road to create a network of ports even to the polar Arctic. Digital infrastructure is also a part of it. But the primary characteristic is that all of these belts and roads end in China at the centre of it all.⁴³

This audacious plan for global domination is based on a theory of history structured around a Marxist interpretation. The discourse is that in ancient times, up until 200 years ago, China was the world's most advanced civilization as the Middle Kingdom to which all other nations and peoples were subordinate.

38 Xing, Guoxin, "Hu Jintao's Political Thinking and Legitimacy Building: A Post-Marxist Perspective".

39 Pomfret, John. "Xi Jinping's Quest to Revive Stalin's Communist Ideology." Washington Post, October 16, 2017, sec. Global Opinions. <https://www.washingtonpost.com/news/global-opinions/wp/2017/10/16/xi-jinpings-quest-to-revive-stalins-communist-ideology/>.

40 Xi, Jinping. "Full Text of Xi Jinping's Report at 19th CPC National Congress." China Daily, November 4, 2017. http://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm.

41 Allison, Graham. "What Xi Jinping Wants." The Atlantic, May 31, 2017. <https://www.theatlantic.com/international/archive/2017/05/what-china-wants/528561/>.

42 Burton, Charles. "MLI's Policy-Maker of the Year: Xi Jinping." Macdonald-Laurier Institute, December 12, 2019. <https://www.macdonaldlaurier.ca/policy-maker-year-xi-jinping/>.

43 Economist author J.P. "The Economist Explains: What Is China's Belt and Road Initiative?" The Economist, May 15, 2017. <http://www.economist.com/blogs/economist-explains/2017/05/economist-explains-11>; Rolland, Nadège. China's Eurasian Century? Political and Strategic Implications of the Belt and Road Initiative. Pentagon Press, 2017.

Then in 1840 China suffered a crushing defeat by the British (“barbarians”) in the first Opium War. From then on China was subject to a succession of imperialistic humiliations, losing control of China’s traditional sovereign territory to Russia, Japan and Western powers. The weakened China becoming known as “the sick man of Asia.” The penultimate humiliation was the transfer of the former German colony in Shandong to the Japanese under the terms of the Treaty of Versailles settlement of World War One, despite the fact that China had supported the Allies in World War One and therefore fully expected that the German colonies would revert to Chinese sovereignty under the terms of the 1919 Paris Treaty.

A significant aspect of Xi Jinping’s program of “the great rejuvenation of the Chinese nation” is to redress the history of humiliations of China by the West. Xi implies that by restoring China to its “rightful place” as the dominant global centre, the West should be put back into a position of subordination.

To achieve this, the Chinese Communist Party has devoted significant resources to its United Front Work Department (UFWD). The mandate of the UFWD is to bring non-Chinese Communist Party elements into collaboration to wittingly or unwittingly serve Chinese Communist Party purposes.⁴⁴

To this end, the regime must identify and cultivate opinion leaders and policymakers that will allow China to realize its geostrategic goals. Covert, coercive, or corrupt means can all be applied to this end. Programs of cyber-espionage are used covertly to obtain information that the regime may use to further economic interest and to plot how to expand political influence in the target country through co-optation of elites. Coercive means can involve blackmail including honey pot temptation operations or threatening of family of the target resident in the PRC. Corrupt means involve the use of psychological cultivation and bribery of persons in key positions in foreign government who can enable China to further its goals.⁴⁵

Gaining support for permitting Huawei to install 5G into national telecommunications systems is so critical to the PRC regime of which Huawei is a part. This is because it has the potential to facilitate massive transfer of data to China that through analysis by sophisticated artificial intelligence algorithms which would allow identification of potential targets for espionage and United Front Work. People dissatisfied with their career progress, with money problems, addictions, etc. who would be more susceptible to approach by agents of the Chinese regime can thus be identified. Or profiles of persons in critical positions can be exploited to cultivate them to serve China’s agendas.⁴⁶

Ultimately Huawei could facilitate PRC knowledge of critical digital infrastructure including key resources such as water, electricity, internet service, etc. The capacity to install kill switches into Huawei digital pipelines would provide China with key advantage. The offering of Huawei technology to China-friendly dictatorial rulers to allow them to sustain their political power by surveillance against potential dissidents and restricting the flow of information to an oppressed people renders them amenable and beholden to China’s authoritarian Chinese Communist Party regime. Huawei thus instrumentally furthers China’s geostrategic strategy to bring about “the community of the common destiny of mankind.”

44 Suzuki, Takashi. “China’s United Front Work in the Xi Jinping Era – Institutional Developments and Activities.” *Journal of Contemporary East Asia Studies* 8, no. 1 (January 2, 2019): 83–98. <https://doi.org/10.1080/24761028.2019.1627714>.

45 Brady, Anne-Marie. “Magic Weapons: China’s Political Influence Activities under Xi Jinping.” *Wilson Center*, September 18, 2017. <https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influence-activities-under-xi-jinping>.

46 Hoffman, Samantha. “Engineering Global Consent: The Chinese Communist Party’s Data-Driven Power Expansion.” *Australian Strategic Policy Institute International Cyber Policy Centre*, January 10, 2019. <https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion>.

4. THE PRC'S HUAWEI STRATEGY TO DOMINATE GLOBAL TELECOMMUNICATIONS

Huawei 3G and 4G equipment has been very successfully marketed to the world's telecommunications concerns because while the quality of the Huawei product is not always the best, it is priced considerably cheaper than the products of its competitors.⁴⁷ As Britain's GCHQ revealed in October 2020, Huawei's "poor software engineering and cyber security processes lead to security and quality issues, including vulnerabilities" which "could include being able to access user traffic or reconfiguration of the network elements."⁴⁸

Huawei has refused to provide answers to direct questions posed by the U.S. House Permanent Select Committee on Intelligence about its financing and relationships with Chinese state banks, nor did it provide documentation or financial records sufficient to audit to test its claims that its sources of financing comply with standard practice and international trade agreements.⁴⁹ The U.S.-China Economic and Security Review Commission has found that enterprises like Huawei rely on generous state-backed financing to make investment projects viable. To the detriment of U.S. competitors, financial subsidies from the Chinese government can enable its national champions, of which Huawei is *primus intra pares*, to penetrate markets by offering products below the costs of production. As a Huawei senior officer has said itself in arguing against the U.S. ban "in many cases, Huawei's is the only equipment that America's small, independent carriers can afford."⁵⁰ This is because of multiple Chinese state subsidies to Huawei. These include hundreds of millions of dollars in grants, heavily subsidized land for facilities, buildings and employee apartments, bonuses to top employees, and massive state loans, such as a \$30 billion credit line with China Development Bank inked in 2009.⁵¹ A 2019 Wall Street Journal review of Huawei's grants, credit facilities, tax breaks and other forms of financial assistance details "how Huawei had access to as much as \$75 billion in state support as it grew from a little-known vendor of phone switches to the world's largest telecom-equipment company — helping Huawei offer generous financing terms and undercut rivals' prices by some 30%."⁵² This figure is also cited in a recent British parliamentary report.⁵³

Huawei also has a history of covertly copying competitors' hardware and software, and purloining proprietary manufacturing processes.⁵⁴ In 2017, a Seattle jury decided that Huawei had misappropriated T-Mobile trade

47 Mcmorrow, Ryan. "Huawei a Key Beneficiary of China Subsidies That US Wants Ended." Agence France Presse. Accessed September 21, 2020. <https://phys.org/news/2019-05-huawei-key-beneficiary-china-subsidies.html>.

48 Martin, Alexander. "GCHQ Discovered 'nationally Significant' Vulnerability in Huawei Equipment." Sky News, October 1, 2020. <https://news.sky.com/story/gchq-discovered-nationally-significant-vulnerability-in-huawei-equipment-12086688>.

49 Almond, Roncevert Ganan. "The Huawei Dilemma: Insecurity and Mistrust," February 4, 2019. <https://thedi diplomat.com/2019/02/the-huawei-dilemma-insecurity-and-mistrust/>.

50 Purdy, Donald A. "Huawei U.S. Security Head: Banning Us Won't Make America Safer." Fortune, June 26, 2018. <https://fortune.com/2018/06/26/huawei-dhs-fcc-china-cyber-security/>.

51 Burton, Charles. "Why Canada Should Not Let Huawei into Our 5G Networks: Debunking Five Myths." Macdonald-Laurier Institute (blog), December 20, 2019. <https://www.macdonaldlaurier.ca/canada-not-let-huawei-5g-networks-debunking-five-myths-charles-burton-inside-policy/>.

52 Yap, Chuin-Wei. "WSJ News Exclusive | State Support Helped Fuel Huawei's Global Rise." Wall Street Journal, December 25, 2019, sec. Tech. <https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736>.

53 Corera, Gordon. "Huawei: MPs Claim 'clear Evidence of Collusion' with Chinese Communist Party." BBC News, October 7, 2020, sec. Technology. <https://www.bbc.com/news/technology-54455112>.

54 For example: Stangel, Luke. "San Jose-Based and Dell and Microsoft Backed Startup CNEX Countersues Tech Giant Huawei, Claiming Attempted IP Theft." Silicon Valley Business Journal, October 19, 2018. <https://www.bizjournals.com/sanjose/news/2018/10/19/cnex-msft-dell-vs-huawei-ip-lawsuit.html>; Plucinska, Joanna. "Poland Arrests Chinese Huawei Employee and Polish National on Spying Allegations." The Independent, January 11, 2019. <https://www.independent.co.uk/news/world/europe/huawei-poland-arrests-spying-china-cyber-security-orange-polska-meng-wanzhou-a8722601.html>;

secrets and awarded the wireless operator \$4.8 million in damages.⁵⁵ Cisco successfully sued Huawei over use of its intellectual property in production of routers (they settled it out of court).⁵⁶ There have long been allegations that Huawei had extensively used espionage against the Canadian firm Northern Telecom that allowed it to benefit from Nortel's research and development and which ultimately contributed to Nortel being forced into bankruptcy in 2009. Huawei has also been accused of providing grants to university research labs in exchange for all the output of the labs' research and development being sent to China as the intellectual property of Huawei.⁵⁷

Huawei has put considerable resources into engaging persons of political influence such as former politicians and senior political staffers to lobby governments to accept Huawei 5G. And there are menacing threats implying economic or other retaliation if governments bar Huawei from 5G networks for security reasons.⁵⁸ Huawei also attempts to bring opinion leaders ("useful idiots") in to counter the prevalent Western media discourse that Huawei is not a private company beholden to the Chinese state but rather an integral element of China's espionage and influence network.⁵⁹ Some commentators have even approvingly quoted a Huawei Canada spokesman's recent claims that, "We're not villains in an espionage thriller. We're a telecom network equipment provider!"⁶⁰

The imperative to have Huawei control global 5G installations is the all-embracing character of 5G connectivity. As cyber security specialists at Auburn University, Frank Ciluffo and Sharon Cardash, put it: "The next generation of wireless technology is expected to fuel even more connectivity in the "internet of things," linking smart cars, smart homes and smart cities together. Billions of devices will be involved, all communicating with each other, forming what could become a surveillance web over much of the planet, and exponentially expanding the number of potential targets for spying."⁶¹

In September 2020, the Toronto Globe and Mail obtained a document drafted by Huawei Canada which lays out commitments that Huawei Canada would undertake if the Government of Canada allows Huawei 5G technology to be adopted by Canada's Bell and Telus and other cellular 'phone service and data providers.⁶² It commits to treat "all confidential information, business and company secrets... obtained under the contract

55 Herman, Arthur. "Huawei's (And China's) Dangerous High-Tech Game." Forbes.com, December 10, 2018. <https://www.forbes.com/sites/arthurherman/2018/12/10/huaweis-and-chinas-dangerous-high-tech-game/#f2db0b211ab7>.

56 Duffy, Jim. "Cisco Sues Huawei over Intellectual Property." Computerworld, January 23, 2003. <https://www.computerworld.com/article/2578617/cisco-sues-huawei-over-intellectual-property.html>.

57 Silcoff, Sean, Robert Fife, and Steven Chase. "Canada's Spy Agency Cautions Universities about Research Ties with Huawei." Accessed September 21, 2020. <https://www.theglobeandmail.com/politics/article-csis-cautions-canadian-universities-about-research-ties-with-huawei/>.

58 Blanchfield, Mike. "Chinese Ambassador Threatens 'Repercussions' on Canada If Huawei 5G Banned - National | Globalnews. Ca," January 17, 2019. <https://globalnews.ca/news/4859737/canada-china-lu-shaye-justin-trudeau-huawei/>; Fullerton, Jamie. "Chinese Ambassador 'threatens to Withdraw Trade Deal with Faroe Islands' in Huawei 5G Row." Accessed October 13, 2020. <https://www.telegraph.co.uk/news/2019/12/11/chinese-ambassador-threatens-withdraw-trade-deal-faroe-islands/>.

59 Fife, Robert. "Inside Huawei's Campaign to Influence Canadian Public Opinion," September 16, 2020. <https://www.theglobeandmail.com/politics/article-inside-huaweis-campaign-to-influence-canadian-public-opinion/>.

60 Olive David. "Five Reasons Canada Should Let Huawei Help Build Our New 5G Networks." Toronto Star, November 26, 2019. <https://www.thestar.com/business/opinion/2019/11/26/five-reasons-canada-should-let-huawei-help-build-our-new-5g-networks.html> in Burton, Charles. "Why Canada Should Not Let Huawei into Our 5G Networks: Debunking Five Myths." Macdonald-Laurier Institute (blog), December 20, 2019. <https://www.macdonaldlaurier.ca/canada-not-let-huawei-5g-networks-debunking-five-myths-charles-burton-inside-policy/>.

61 Ciluffo, Frank J., and Sharon L. Cardash. "What's Wrong with Huawei, and Why Are Countries Banning the Chinese Telecommunications Firm?" The Conversation, May 16, 2019. <http://theconversation.com/whats-wrong-with-huawei-and-why-are-countries-banning-the-chinese-telecommunications-firm-109036>.

62 Fife, Robert, and Steven Chase. "Huawei Canada Draws up 'No-Backdoor No-Spying' Legal Pledge in Bid to Prevent 5G Ban." Globe and Mail, September 17, 2020. <https://www.theglobeandmail.com/politics/article-huawei-canada-draws-up-no-backdoor-no-spying-legal-pledge-in-bid-to/>.

relationship as confidential," and says "all confidential information will not be transferred to a third party or used for purposes other than those stipulated in the contract without the consent of the carrier." "Huawei agrees no information shall ever be provided to any foreign intelligence agency outside of Canada... Huawei agrees to never implant or allow others to implant in its equipment, or to collect intelligence for any individual or organization, including any government organizations, agencies and entities" and "confirms that it has never had any legal or moral obligations to implant or allow others to implant espionage, communications kill switches or other malicious functionalities (backdoor) to its equipment." The document obliges Huawei to allow its 5G equipment to be tested independently for backdoors. Canadian security officials currently test Huawei 4G gear at independent labs. But tellingly governments in Canada are not permitted to use Huawei equipment. Huawei is the only foreign telecommunications equipment maker that faces such requirements in Canada.

In 2018, the Czech National Cyber and Information Security Agency issued a warning against the use of Huawei's software and hardware as products posing a security risk and in the fall of 2020 Huawei was denied security clearance from the country's National Security Authority necessary to participate in selected public tenders in the Czech Republic.⁶³

U.S. and Australian government officials have warned Canada that China could use Huawei's equipment to spy on other countries because China's 2017 National Intelligence Law gives Beijing authority to order Chinese companies to carry out espionage for national security purposes.⁶⁴ This document attempts to assure the Canadian government that the Canadian subsidiary would reject any such demand. Considering the record of Huawei in its violation of contracts, theft of I.P., and well borne out allegations of fraud by Huawei's senior management, there is a high degree of scepticism over the integrity of Huawei Canada's "no spying" commitment. Moreover, there are no provisions for sanctions should Huawei Canada be found to be engaging in activities at odds with these commitments.

63 Česká televize. "Huawei bezpečnostní prověrku v Česku nedostane, píše Deník N." ČT24 - Nejdůvěryhodnější zpravodajský web v ČR - Česká televize, September 15, 2020. <https://ct24.ceskatelevize.cz/ekonomika/3184296-huawei-bezpecnostni-proverku-v-cesku-nedostane-pise-denik-n>.

64 Canadian Security Intelligence Service. "China's Intelligence Law and the Country's Future Intelligence Competitions." , May 10, 2018. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html>.

While the United States urges all nations of the world to ban the use of Huawei equipment from their networks, the U.S. intelligence gathered to proffer the evidence supporting this claim has to be kept from public disclosure because it is classified.



5. WHAT WE KNOW ABOUT U.S. INTELLIGENCE ON HUAWEI'S 5G CHALLENGE TO DOMESTIC AND GLOBAL SECURITY

In May 2019, U.S. President Donald Trump issued an “Executive Order on Securing the Information and Communications Technology and Services Supply Chain.”⁶⁵ The order shows “foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people. I further find that the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.”

In February 2018, the heads of the CIA, FBI, NSA and the U.S. Director of National Intelligence indicated to the U.S. Senate Intelligence Committee that private citizens should not use products from Chinese companies. FBI Director Christopher Wray testified that he is deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share U.S. values to gain positions of power inside U.S. telecommunications networks that provides the capacity to exert pressure or control over telecommunications infrastructure or provides the capacity maliciously to modify or steal information or provide the capacity to conduct undetected espionage.⁶⁶ The U.S. is concerned about “the potential loss of control over U.S. ‘critical infrastructure’; the interdependent system of electric power grids; banking and finance systems; natural gas, oil, and water systems; and rail and shipping channels — each of which depend on computerized control systems.” The U.S. House Permanent Select Committee on Intelligence has further concerns over Chinese motivations and their capacity to maliciously modify or steal information from government and corporate entities in order to gain access to expensive and time-consuming research and development that would advance China's economic position on the world stage.⁶⁷

In 2018, the U.S. Department of Justice indicated in a report to the U.S. Senate Intelligence Committee that “from 2011-2018, more than 90 percent of the Department's cases alleging economic espionage by or to benefit a state involve China, and more than two-thirds of the Department's theft of trade secrets cases have had a nexus to China.”⁶⁸

The United States has indicated to its allies and to the world that it has evidence that Huawei poses a severe security threat to global telecommunications wherever its hardware and software solutions are installed. Allegations that Huawei steals data and transfers it to China have not been publicly substantiated. But while the United States urges all nations of the world to ban the use of Huawei equipment from their networks,

65 Trump, Donald J. “Executive Order on Securing the Information and Communications Technology and Services Supply Chain.” 5/19/2020. The White House. Accessed September 20, 2020. <https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>.

66 Salinas, Sara. “Six Top US Intelligence Chiefs Caution against Buying Huawei Phones.” CNBC, February 13, 2018. <https://www.cnbc.com/2018/02/13/chinas-huawei-top-us-intelligence-chiefs-caution-americans-away.html>.

67 Almond, Roncevert Ganan. “The Huawei Dilemma: Insecurity and Mistrust,” February 4, 2019. <https://thediplomat.com/2019/02/the-huawei-dilemma-insecurity-and-mistrust/>.

68 Maza, Cristina. “China Is Involved in 90 Percent of Espionage, Department of Justice Reveals.” Newsweek, December 12, 2018. <https://www.newsweek.com/china-involved-90-percent-economic-espionage-and-industrial-secrets-theft-1255908>; Lucas, Ryan. “U.S. Charges Alleged Chinese Government Spy With Stealing U.S. Trade Secrets.” NPR.org, October 10, 2018. <https://www.npr.org/2018/10/10/656280811/u-s-charges-alleged-chinese-government-spy-with-stealing-u-s-trade-secrets>.

for operational reasons, the U.S. intelligence gathered to proffer the evidence supporting this claim has to be kept from public disclosure because it is classified.⁶⁹ This leads to doubt among those who lack confidence in the honesty and integrity of the United States, particularly under the current presidency of Donald Trump.⁷⁰ But nevertheless there is a high degree of consensus among intelligence specialists around the world that the US claims of Huawei's unreliability are highly credible. Banning Huawei is not simply acceding to a U.S. demand, but critical to the preservation of all nations' national security. Australia, for example, made such a determination in 2018 prior to the Presidential Executive Order cited above.⁷¹ Indeed, there is no smoking gun needed. If opportunity and intent is given, untrustworthy actors to whom Huawei is beholden will use this access, especially in a crisis. Access is the hardest part of hacking. Access is strategic capability.⁷²

The U.S. has also made it clear to its Five Eyes Intelligence Alliance that the U.S. cannot entrust secret information to any partner that allows Huawei 5G into its national telecommunications network. This is critical in the case of Canada because of the high degree of integration of North American telecommunications.⁷³

69 Kingsbury, Alex. "Why Classified Secrets Should Be Kept From the Public." US News & World Report, June 11, 2010. <https://www.usnews.com/opinion/articles/2010/06/11/why-classified-secrets-should-be-kept-from-the-public>.

70 Guthrie, Douglas. "Protectionism Is Not Patriotism—And It's Putting the Economy at Risk." US News & World Report, November 19, 2012. <https://www.usnews.com/opinion/articles/2012/11/19/protectionism-is-not-patriotism-and-its-putting-the-economy-at-risk>.

71 Kaye, Byron, and Kaye Westbrook. "China's Huawei Slams Australia 5G Mobile Network Ban as 'Politically Motivated.'" Reuters, August 24, 2018. <https://www.reuters.com/article/us-australia-china-huawei-tech-idUSKCN1L72GC>; Uchill, Joe. "Report: Australian Intelligence Knows Huawei Was Used in Espionage." Axios, November 4, 2018. <https://www.axios.com/report-australian-intelligence-know-huawei-1541285886-42f1eb64-98de-422f-9686-4174e41ef37e.html>.

72 Gilding, Simeon. "5G choices: a pivotal moment in world affairs." The Strategist, January 29, 2020. <https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/>.

73 CTV News Staff. "A Real Risk: U.S. Warns Allies against Allowing Huawei in 5G Networks." CTV News. Accessed March 30, 2019. <https://www.ctvnews.ca/politics/a-real-risk-u-s-warns-allies-against-allowing-huawei-in-5g-networks-1.4307754>.

6. U.S. MEASURES TO CONTAIN HUAWEI AND THE PRC'S COUNTERMEASURES

In July 2020 the U.S. announced it had imposed travel bans on employees of Huawei and other Chinese companies the U.S. determines are assisting authoritarian governments in cracking down on human rights, including in China's Xinjiang Uyghur Autonomous Region.⁷⁴

Having determined that Huawei poses a severe threat for the security of telecommunications, the United States has adopted measures to prevent U.S.-developed technology from benefiting Huawei. This has included restricting the sale of chips exported to China for use in manufacture of Huawei hardware.⁷⁵ For example in September 2020 the United States enacted a ban that prohibits any company from selling semi-conductors to Huawei that rely on U.S. hardware or design software. So Japanese firms such as Sony, Kioxia and Renesas, which had supplied an estimated US\$14.4-billion in parts to Huawei in 2019, stopped shipments in mid-September 2020. Unless some resolution is made, Huawei could be short of critical components to manufacture handsets and 5G network hardware by early in 2021.⁷⁶ The inability to obtain these cutting-edge chips will wipe out billions of dollars of sales for Huawei's and its status as number one smartphone maker in the world will be threatened.⁷⁷ Richard Yu, president of Huawei's consumer unit indicated last summer that production of Kirin chips designed by Huawei's own engineers would stop Sept. 15 because they are made by contractors that need U.S. manufacturing technology. According to a video recording of his comments made at an industry conference, China Info 100, Mr. Yu said Huawei lacks the ability to make its own chips. "This is a very big loss for us. Unfortunately, in the second round of U.S. sanctions, our chip producers only accepted orders until May 15. Production will close on Sept. 15. This year may be the last generation of Huawei Kirin high-end chips." More broadly, Huawei's smartphone production has "no chips and no supply." Yu said this year's smartphone sales probably will be lower than 2019's level of 240 million handsets.⁷⁸

And the U.S. has taken action to deny Huawei access to Google Android apps. Because Huawei cannot manufacture its equipment using Chinese chips, nor duplicate the variety quantity and quality of Android apps available through Google, these measures are crippling to Huawei's global competitiveness.⁷⁹

74 Lee, Matthew. "US to Hit Huawei Employees with Visa Bans for Rights Abuses." Washington Post, July 15, 2020. https://www.washingtonpost.com/business/technology/us-to-hit-huawei-employees-with-visa-bans-for-rights-abuses/2020/07/15/08c6720a-c6ac-11ea-a825-8722004e4150_story.html.

75 BBC News. "Huawei: US Tightens Restrictions on Chinese Giant." BBC News, August 17, 2020, sec. Business. <https://www.bbc.com/news/business-53805038>.

76 Vanderklippe, Nathan. "As U.S. Ban Takes Effect, Retailers in China Report Slowing Supplies of Huawei Phones." Globe and Mail, September 16, 2020. <https://www.theglobeandmail.com/world/article-as-us-ban-takes-effect-retailers-in-china-report-slowing-supplies/>.

77 Kharpal, Arjun. "Huawei Options as U.S. Sanctions Cut Its Supply of Smartphone Chips." CNBC.com, August 11, 2020. <https://www.cnbc.com/2020/08/12/huawei-options-as-us-sanctions-cut-its-supply-of-smartphone-chips.html>.

78 McDonald, Joe. "Huawei: Smartphone Chips Running out under US Sanctions." AP NEWS, August 8, 2020. <https://apnews.com/article/smartphones-technology-business-ap-top-news-china-270e93e985733a4d086c06a01375cea0>.

79 Byford, Sam. "Living a Google-Free Life with a Huawei Phone." The Verge, March 25, 2020. <https://www.theverge.com/2020/3/25/21193639/huawei-mate-30-google-apps-services-appgallery-p40-preview>.

CONCLUSION: THE FUTURE OF HUAWEI 5G IN CHINA'S GEOSTRATEGY AND THE WEST'S RESPONSE

China's extreme response⁸⁰ to the detainment of the Huawei CFO Meng Wanzhou on serious charges of fraud is indicative that the Huawei CFO is not simply a senior official of a multinational corporation headquartered in China, but that Meng Wanzhou is a senior member of the Chinese regime. Despite Ms. Meng having been charged in a U.S. court some months before, China did not expect the Canada would actually arrest such a high-ranking person in response to a U.S. extradition request. China's Ambassador to Canada at the time, Lu Shaye, said that the arrest of Meng was an act of "backstabbing" by a friend.⁸¹ The Chinese Foreign Ministry has indicated that Canada's arrest of Ms. Meng at the request of the U.S. while she was changing planes in Vancouver was "extremely nasty."⁸² Moreover as Ms. Meng could be facing a very long prison term in the United States if convicted of multiple charges,⁸³ PRC could well be concerned that she would cut a deal for leniency by revealing to the US authorities the relationship between Huawei and Chinese security and intelligence agencies and the People's Liberation Army.⁸⁴

Chinese official statements express a great deal of anger over the Meng arrest. Perhaps this is reflective of Chinese resentment over its Huawei plans increasingly being foiled. More canny awareness of Xi Jinping's geostrategic agenda in the U.S. and the rest of the West, by China overplaying its hand, the PRC disassembling disassembling over COVID-19, and ugly "Wolf Warrior diplomacy" and incredible disinformation. is making it harder and harder for China to realize its deeper stealthy agenda of global hegemony.

U.S. action may indeed cause Huawei to fail as a viable global entity.⁸⁵ But the overall scheme of the Belt and Road Initiative buttressing an eventual Chinese global hegemony under the rubric of the community of the common destiny of mankind will endure past Huawei as a single contributing component. The PRC's urgency to redress the humiliations of past history remains a key motivator in the PRC's nationalist psyche. The critical imperative to gain control of global telecommunications to serve China's audacious global ambitions is deeply embedded in the legitimating mission of the Chinese Communist Party. If it is not Huawei, one could expect that one day in the future when PRC has retrenched to self-sufficiency in production of the hardware and software necessary to dominate over all international competitors in telecommunications networks throughout the world, that possibly under a different corporate name, the regime will reapply its ambition to dominance and control over global telecommunications to further strive to realize its China dream of the of the great rejuvenation of the Chinese nation.

The scenario of Xi Jinping's grand vision of great rejuvenation of the Chinese nation and China's resultant global hegemony under the authoritarian rule of the Chinese Communist Party would imply the end of freedom and democracy for all nations of the world clinging to it in this troubled age. But the achievement of Xi Jinping's plan to achieve a China-centred trade and investment Belt and Road and a community of the

80 Forrest, Adam. "China Warns Canada of 'severe Consequences' over Huawei Chief's Arrest." The Independent, December 8, 2018. <https://www.independent.co.uk/news/world/americas/huawei-arrest-china-canada-meng-wanzhou-us-a8673921.html>.

81 Blanchfield, Mike. "Chinese Ambassador Threatens 'Repercussions' on Canada If Huawei 5G Banned - National | Globalnews. Ca," January 17, 2019. <https://globalnews.ca/news/4859737/canada-china-lu-shaye-justin-trudeau-huawei/>.

82 Forrest, Adam. "China Warns Canada of 'severe Consequences' over Huawei Chief's Arrest." The Independent, December 8, 2018. <https://www.independent.co.uk/news/world/americas/huawei-arrest-china-canada-meng-wanzhou-us-a8673921.html>.

83 U.S. Department of Justice. "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud," January 28, 2019. <https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial>.

84 Balding, Christopher. "Huawei Technologies' Links to Chinese State Security Services." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 5, 2019. <https://doi.org/10.2139/ssrn.3415726>.

85 Miller, Chris. "America Is Going to Decapitate Huawei." New York Times, September 15, 2020. <https://www.nytimes.com/2020/09/15/opinion/united-states-huawei.html>.

common destiny of mankind is not written in stone.⁸⁶ There are many unknown factors that could scotch Mr. Xi's Chinese Communist Party's domestic and global agenda. Chinese history and culture can be read in many ways.⁸⁷ In Leninist states, the future is uncertain, and the past is always changing. China's future political leadership could reinterpret China's past and China's national future aspirations to re-legitimize itself as a democratic responsible stake holder in global affairs.

One can only hope that domestic factors in China will eventually lead to a democratic regime compatible with the existing rules-based order and the economic systems of liberal free-market economies.⁸⁸ Under those conditions, China could become a major force for technological innovation, prosperity and justice throughout the world.

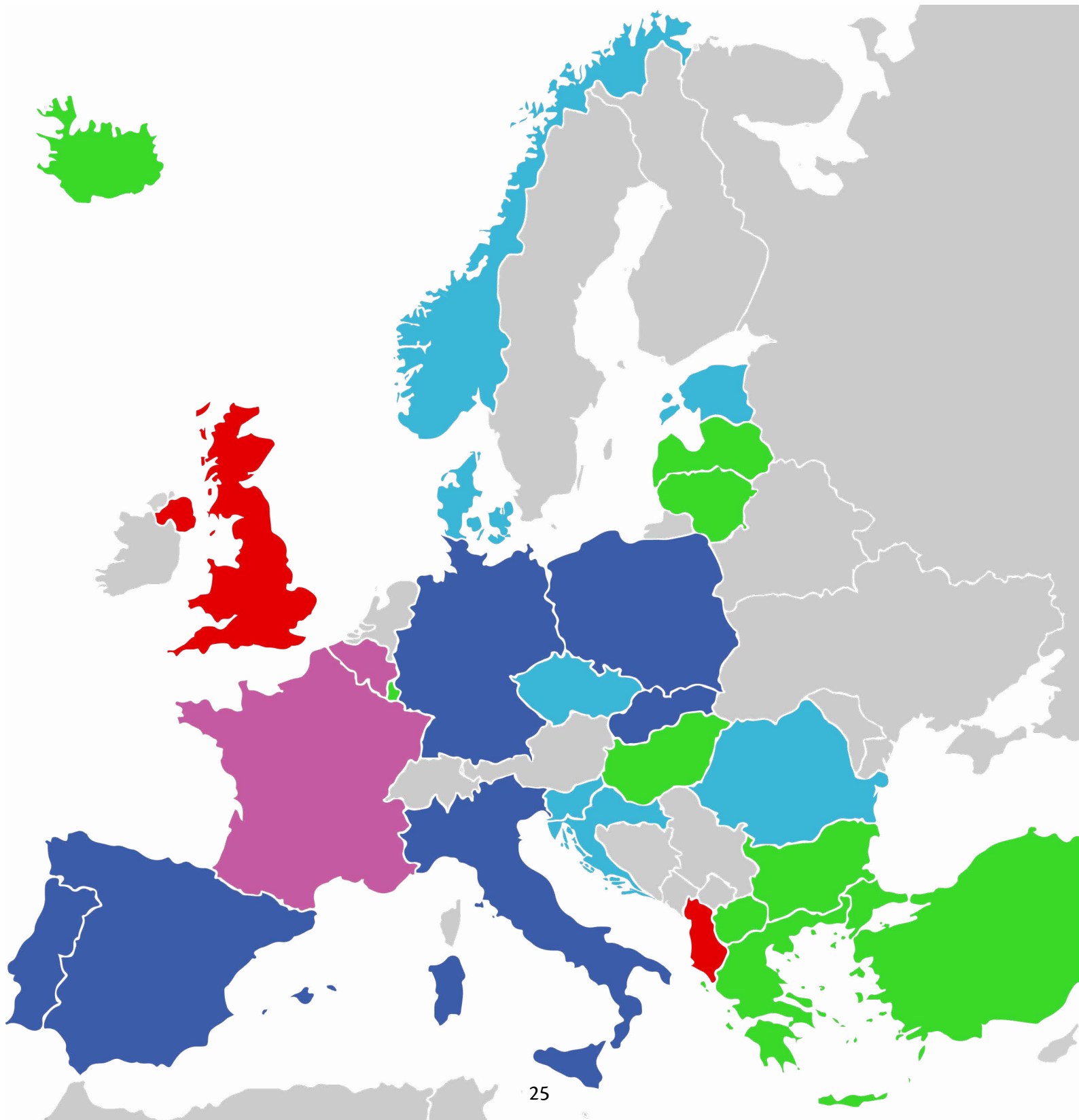
86 Holland, Tom. "Why China's 'One Belt, One Road' Plan Is Doomed to Fail." South China Morning Post, May 1, 2017. <http://www.scmp.com/week-asia/opinion/article/1999544/why-chinas-one-belt-one-road-plan-doomed-fail>.

87 Burton, Charles. "The Chinese Communist Party Is Not Really Very Chinese at All." Globe and Mail, July 3, 2020. <https://www.theglobeandmail.com/opinion/article-the-chinese-communist-party-is-not-really-very-chinese-at-all/>.

88 Shambaugh, David. "The Coming Chinese Crackup." Wall Street Journal, March 6, 2015, sec. Life. <http://www.wsj.com/articles/the-coming-chinese-crack-up-1425659198>.

APPENDIX: NATO STATES RESPONSE TO 5G & HUAWEI (COMPILED BY THE EUROPEAN VALUES CENTER FOR SECURITY POLICY)

Allowed	On the fence	Unlikely to use	Restrictions	Ban in effect
---------	--------------	-----------------	--------------	---------------



Allowed	On the fence	Unlikely to use	Restrictions	Ban in effect
---------	--------------	-----------------	--------------	---------------

State	Current corporates' stance on Huawei's 5G and status of infrastructure developments (halted/ongoing buildings/previous projects with Huawei)	Policy-making response (adopted policies, laws, officials' statements)
Bulgaria (no decision yet)	<ul style="list-style-type: none"> As 5G is not yet commercially launched, no companies are launching 5G services yet. However, the three operators in the Bulgarian market – A1 Bulgaria, Telenor and Vivacom – are preparing to provide 5G services in the course of 2020/2021. All three telecoms operators held successful 5G tests and demonstrated 5G operating in their networks, thus confirming that their infrastructure is ready to provide 5G services. Mobile operators expect the deployment of the new frequency resource at the beginning of 2021, and the government expects to implement 5G within a five-year period. The original plan was to offer 5G frequencies by June 2020, but it got delayed because of the coronavirus pandemic and other factors. 	<ul style="list-style-type: none"> According to publicly available information, Nokia, Alcatel and Huawei are interested in the development of the 5G infrastructure. In one of the 5G trials in July 2019, Telenor was going to use Huawei equipment, which includes both fixed base stations, as well as a mobile base station that can be transported across the country.
Greece	<ul style="list-style-type: none"> Ericsson has been selected as sole 5G radio access network (RAN) supplier by Cosmote, the mobile arm of the Hellenic Telecommunications Organisation (OTE) and Greece's largest mobile communications service provider. 	<ul style="list-style-type: none"> Cosmote says its 5G network rollout, which was due to begin in May, will be impacted by the COVID-19 pandemic. The rollout may be delayed up to four months. Greece has shown reluctance to use the Huawei Fifth Generation because of US pressure.
Hungary	<ul style="list-style-type: none"> Magyar Telekom, Hungary's biggest telecommunications company, and Ericsson launched commercial 5G in Hungary in April, 2020. On March 26, 2020, Magyar Telekom secured the related 3.5GHz spectrum in Hungary's spectrum auction. The license will expire in 2035. 	<ul style="list-style-type: none"> Operators will have the option to extend access to the spectrum usage rights for five years after the initial period expired, for an additional one-off payment.
Iceland	<ul style="list-style-type: none"> One of Iceland's major mobile operators, Nova, began conducting 5G tests in 2019. In May 2020, Iceland allocated 5G frequencies. 	<ul style="list-style-type: none"> Nova signed an agreement to partner with Chinese company Huawei in 5G deployment in February 2019. Nova invested a billion krónur in development of its network in 2018 and the company planned to invest around a billion krónur more in 2019
Latvia	<ul style="list-style-type: none"> On July 19 2019, Latvia's 5G communication network was officially launched by the President of Latvia, Egils Levits. The first 5G Tech Forum (5G Techritory) was held in Latvia in September 2018. The 5G network has been in "test mode" for 9 months before launch. It is now available to anyone with a device supporting 5G technology. 	<ul style="list-style-type: none"> The Latvian mobile operators "Latvian Mobile Telephone" (LMT) and TELE2 offer full access to the 5G network. In February 2020, Latvia and the US signed a joint declaration signed by on 5G network security. "Such efforts will not only improve national security, but also provide opportunities for private sector innovators to succeed under free and fair competition and benefit our respective digital economies," the declaration says.

Lithuania	<ul style="list-style-type: none"> In September 2018, the government announced that it planned to run an auction for 700 MHz frequencies by 2022 after the government decided to free the band, which was used for digital TV, for 5G. In 2019, Lithuania prepared to launch its frequencies auction for its 5G network in early 2020, despite calling on the EU to create a blacklist of telecommunication companies and include a cybersecurity clause in its tenders. By 2025, the 5G network should cover urban territories, international land transport corridors (Via Baltica, Rail Baltica) and other highways, main railway lines, airports and seaports. 	<ul style="list-style-type: none"> In June 2020, Lithuania announced that 5G would rollout in 4 stages: Beginning of implantation of 5G connection and its development in the domestic territories in 2021; 5G connection is available in at least one of the largest Lithuanian cities by 2022; Uninterrupted 5G functioning in Vilnius, Kaunas, Klaipeda, Siauliai and Panevezys by 2023; 5G connection is available in the territories of towns and villages, international transport corridors ("Via Baltica", "Rail Baltica"), on the roads of national importance, on the railways and in the ports by 2025.
Luxembourg	<ul style="list-style-type: none"> Testing of 5G technology is currently underway, but full commercial deployment is unlikely before 2022. 	<ul style="list-style-type: none"> In July 2020, the Director of the Luxembourg Institute of Regulation announced that a 5G network should be in place by the end of 2020. The 700 MHz band should cover 50% of the country by 2022, and 90% by 2024.
North Macedonia	<ul style="list-style-type: none"> By the end of 2023, 5G signal should be available on the territory of at least one city in North Macedonia. "Even though no telcos and communication players have launched 5G services yet the two biggest mobile network operators, Makedonski Telekom and One.Vip, have announced that they will be launching 5G services as of 2020." 	<ul style="list-style-type: none"> North Macedonia's regulator, the Agency for Electronic Communications (AEK), is planning to award 5G spectrum in the second half of this year and has opened a public consultation on the initiative.
Turkey	<ul style="list-style-type: none"> Turkey has welcomed Huawei's 5G. 2020: Chinese technology giant Huawei will pursue further investments in Turkey and it will not be deterred by global circumstances, according to a senior official of Huawei Turkey. 2017: Turk Telekom signs an MoU with Huawei announcing they will cooperate to develop 5G technology. 2017: Turkcell and Huawei test 5G technology in Istanbul. 	<ul style="list-style-type: none"> Turkey is a critical hub for developing the Huawei Mobile Services (HMS) ecosystem. Not banned, no restrictions adopted on the legislative level.

Canada	<ul style="list-style-type: none"> 5G service rolled out by Rogers is technically already available in Vancouver, Calgary, Edmonton, Toronto, Ottawa and Montreal with dozens more markets expected to launch before the end of 2020. More cities were covered this year by Bell and Telus. Still in February 2018, Huawei carried out successful trials with Bell and Telus, but in September 2018 The Communications Security Establishment intelligence agency said it had been conducting tests on Huawei equipment since 2013 to see if it poses any danger to the country. 	<ul style="list-style-type: none"> All major telecom companies in Canada (Rogers, Bell, Telus) plan to use European suppliers for 5G, specifically the equipment from Scandinavian component makers Nokia and Ericsson. Canada is listed among the countries who support the US Department of State initiative "The Clean Network" However, according to Reuters, "Canada is the only member of the Five Eyes intelligence-sharing network that has not formally blocked Huawei from 5G networks, but it has effectively done just that, delaying a decision long enough to force telecom companies to exclude the Chinese gear maker". Huawei Chief Financial Officer, daughter of the founder and president of Huawei, Meng Wanzhou is fighting extradition to the United States since Canadian police detained her in December 2018. In response, Beijing arrested Canadian citizens Michael Spavor and Michael Kovrig, charging them with espionage. Canada says gaining their freedom is a top priority. "If it weren't for the two Michaels, Canada would have already said it would not be using Huawei 5G technology," a diplomatic source said.
Germany	<ul style="list-style-type: none"> In June 2020, Deutsche Telekom said it already has 12,000 5G antennas live, with 40,000 expected on air by the end of 2020. 5G services are available in more than 1,000 towns and DT is tracking to reach 50% of Germany's population, or 40 million people by mid-July. For its 5G radio access network (RAN), the operator was continuing to use gear from existing 4G suppliers Ericsson and Huawei. 	<ul style="list-style-type: none"> Vodafone Germany and Huawei started 5G assessment tests back in 2016. In February 2017, Deutsches Zentrum fuer Luft- und Raumfahrt (the German Aerospace Center) signs a collaboration agreement with Huawei to define requirements on future 5G mobile radio standards for use cases and 5G automotive applications. In October 2017, Deutsche Telekom and Huawei announce the implementation of 5G antennas in Berlin. In February 2019, Angela Merkel set out conditions to ensure Huawei participation in German 5G network is safe. In March 2019, Germany toughens security criteria for all telecoms equipment vendors, and in October - publishes new security guidelines on 5G networks Deutsche Telekom said no telecoms equipment vendor should be barred from Germany on political grounds, reiterating its opposition to calls from some lawmakers to bar China's Huawei Technologies on national security grounds, according to Reuters. "Debate continues in Berlin over whether to bar China's Huawei Technologies from the German market." And regardless of politics, the roll out of German 5G network will not rely on a single provider. Deutsche Telekom "promised to phase out" Huawei from the core network, however. Ericsson was chosen over Huawei as the core network provider for Telefónica Deutschland. More updates are expected in September.

Italy	<ul style="list-style-type: none"> • A 5G trial was launched in March 2017 to implement infrastructures and services in 5 cities: the metropolitan area of Milan, Prato, L'Aquila, Bari, and Matera. • In September 2017, assignments of the permission to use the 100 Mhz in the portion of spectrum between 3.6-3.8 Ghz to experience 5G in 5 Italian cities have been authorised. 	<ul style="list-style-type: none"> • Italy held auctions at the end of 2018 raising over 6.55 billion euros (\$7.3 billion).
Poland	<ul style="list-style-type: none"> • Previously, local telecom operators procured Huawei equipment for their rollout of previous generations of internet networks and has been heavily reliant on Chinese provider Huawei due to its low prices, but the government has since turned sceptical of relying on Chinese kit. • "Poland is trying to diversify 5G suppliers to balance its own interests". In this way, Warsaw strives to avoid a direct confrontation with Beijing in the style of Trump's administration, but the relationship with Washington is still of the utmost importance • Play, Poland's biggest mobile operator, has also warned that a complete ban on Huawei could raise prices and limit technological development, telling Reuters that they had not found any security issues with the equipment. 	<ul style="list-style-type: none"> • 2020: Poland is working on a telecom security law that will further toughen controls that would "limit the use of [telecom equipment] vendors who are suspicious or who are not necessarily trustworthy, or who do not stick to the security standards, according to the Digital Minister Marek Zagórski • 2019, April: Poland is unlikely to exclude all Huawei equipment from its next-generation mobile networks, a government minister told Reuters, in part to avoid increased costs for mobile operators. • 2019: Huawei has been a sensitive issue in Sino-Polish relations since January 2019, when Polish authorities last year also arrested two telecom officials in an investigation into alleged espionage on behalf of Chinese security services, one of whom, Wang Weijing, worked for Huawei in Poland. • September 2019: Warsaw signed an agreement with the U.S. government pledging to only allow "trusted" suppliers into 5G networks. Huawei was not named in the joint declaration; equipment suppliers for 5G networks should be carefully evaluated to determine "whether the supplier is subject, without independent judicial review, to control by a foreign government."
Portugal	<ul style="list-style-type: none"> • 2020: The three companies who dominate Portugal's mobile phone market (NOS (NOS.LS), Vodafone (VOD.L) and Altice (ATCA.AS) said they would not use Huawei technology in their core 5G networks despite the government not banning the Chinese group from supplying critical infrastructure. • Neither company gave a reason for not using Huawei in their core networks. Their stances potentially leave the door open for them to use Huawei in non-core parts of the 5G rollout. • Portugal postponed its 5G spectrum auction for six months to October due to the coronavirus pandemic. 	<ul style="list-style-type: none"> • The Portuguese government has so far not taken a stance, but Infrastructure Minister Pedro Nuno Santos told Reuters it has "no 'a priori' issues with any manufacturer". • A group created by the Portuguese government to assess risks and cybersecurity issues relating to 5G had completed its work and had not drawn any conclusions directed against any particular supplier. • 2019: Portugal is the latest western country to say it won't ban Huawei from its 5G network, while Telefónica Spain is using Huawei for its 5G core. • 2019: Portugal formally notified the US it won't be excluding any Chinese vendors from participation in its 5G network. The report goes on to note that Portugal already has a fair bit of Chinese infrastructure investment and may be wary of putting that sort of thing in jeopardy.

Slovakia	<ul style="list-style-type: none"> • 2020: Four Slovak mobile operators decide on suppliers for future 5G networks. The only operator who has it clear already is Orange. It announced cooperation with Nokia, reported Zive.sk. Slovak Telekom has not taken any decision yet. O2 Slovakia runs a tender to select a supplier. • Finally, the fourth MNO 4ka admits being in touch with four suppliers: ZTE, Nokia, Huawei and Ericsson. • Orange Slovensko announced its decision to rely on Nokia as a 5G technology supplier. In particular, the operator does not count on Huawei equipment in any part of its network. • 2019 the Slovak branch of Huawei Technologies Ltd. recently participated in a public debate for the preparation and implementation of tenders 	<ul style="list-style-type: none"> • 2019: Slovakia has no evidence of Huawei security threat - prime minister. The gov would need evidence the company's technology poses a risk before imposing any restrictions.
Spain	<ul style="list-style-type: none"> • Telefónica's existing 4G technology in Spain depends entirely on Huawei equipment so Telefónica will continue to have Huawei technology in what is known as its 5G core – where the most sensitive information is stored – for now and in its so-called periphery, which consists of masts, antennas and passive equipment. • 2020: Telefónica said it would reduce the amount of Huawei kit in new networks (but still procure the Chinese vendor), while Orange said it would use ZTE, Huawei and Ericsson in Spain. • Spain's biggest telecommunications companies, including Telefonica and Vodafone, say they have taken steps to reduce Chinese input for their core systems of future data management in mobile telephones. • February, 2020, Pressure from the U.S: U.S. officials warned Spanish officials and telecommunications executives that the U.S. could stop sharing sensitive information with Spain if the Chinese firms reportedly involved in 5G technology were not excluded from local markets. • December 2019: Spanish telecom giant Telefonica has awarded part of the contract to deploy its 5G core network to Chinese vendor Huawei. Telefonica also intends to award that contract to a different supplier, so as not to depend solely on Huawei for its network deployment. Telefonica had previously awarded to Huawei a contract for the deployment of its core 4G network, according to the report. • June 2019: In cooperation with Chinese telecom giant Huawei, Vodafone Espana on Saturday rolled out the first commercial 5G mobile services in Spain. 	<ul style="list-style-type: none"> • 2020: Spain's national intelligence service certified the software of Huawei as safe and compliant with the relative legislation last month. • 2020: The economy minister in February said she was preparing legal acts, but the country since then faced delays and had to push back a spectrum auction due to the pandemic. • In 2019 the Spanish National Cryptologic Center, for instance, warned in its 2019 annual report that Chinese attacks targeted critical infrastructure to gather information about possible vulnerabilities and used spear-phishing to conduct cyber espionage in order to acquire technological capacity and economic and security intelligence.
Croatia (basically will not use)	<ul style="list-style-type: none"> • Croatia's communication service provider Hrvatski Telekom (HT) has selected Ericsson Nikola Tesla as its sole supplier of 5G Radio Access Network (RAN) products and services until 2024, over "less trusted" vendors. • The Government has also chosen Osijek as a 5G City where the commercial work on 5G technology will begin by the end of 2020. • Not all of the preconditions have been created for construction, not only in the form of permits but also free frequencies and the spread of devices that could support the new network. 	<ul style="list-style-type: none"> • In January 2020, U.S. "warned" Croatia to "be careful when choosing 5G network equipment".

Czech Republic		<ul style="list-style-type: none"> Czech Republic is listed among the countries who support the US Department of State initiative "The Clean Network". On May 6 the Czech Republic and the US have signed a Joint Declaration on 5G Security. However, as per August 13, during the meeting with Mike Pompeo, Andrej Babiš announced that the decision on Huawei's engagement in the 5G future is yet to be made and will take place within the EU framework. In September 2020 should take place the Prague 5G Security Conference where further discussions are expected to continue.
Denmark	<ul style="list-style-type: none"> Denmark started the rollout of 5G in 2019, and according to TDC Net, which is responsible for the physical infrastructure in the company's mobile network, 80% of Denmark will be covered by 5G networks before the end of September, and before the end of 2020 it will be covering 90% of the country. 	<ul style="list-style-type: none"> In May 2018, Denmark's biggest single telecoms operator TDC tested 5G technology in partnership with Huawei. Last year, TDC picked Ericsson over Huawei for its 5G network. In June 2020, Danish Minister of Defense Trine Bramsen claimed that Denmark "would like to rely on 5G suppliers based in allied countries rather than other potential suppliers". Denmark is listed among the countries who support the US Department of State initiative "The Clean Network".
Estonia	<ul style="list-style-type: none"> 5G should be standardized by 2020. By 2023 they expect it in major cities. 4G and 5G will work in symbiosis, and in 2025 Estonia plans to have a 4G/5G network that has features from both generations. 	<ul style="list-style-type: none"> The Ministry of Economic Affairs and Communications is preparing a regulation which would allow restrictions on use of high-risk technologies in telecoms networks. For instance, Huawei from Estonia's 5G network. The entry into force of the restrictions is also a precondition for moving forward with the 5G frequency licensing competition. In late 2019, Prime Minister Jüri Ratas met with US Vice President Mike Pence to reach agreement on a joint Estonian-U.S. approach to 5G and its security, based on the "shared principles". Elisa is the only mobile telephone operator in Estonia which has not ruled out using Huawei's technology in its 5G networks. The other two, Telia and Tele2 have said they would opt for Nokia or Ericsson. Estonia is listed among the countries who support the US Department of State initiative "The Clean Network".
Norway	<ul style="list-style-type: none"> Norwegian telecoms firm Telenor (state-controlled) announced that it would use Sweden's Ericsson to build the country's next-generation 5G networks, gradually removing China's Huawei after a decade of collaboration over 4G. Telenor will still use Huawei to maintain 4G and also upgrade to 5G coverage in selected areas of Norway. 	<ul style="list-style-type: none"> September 2019: Norway does not plan to block China's Huawei Technologies from building the country's 5G telecoms network, cabinet minister Nikolai Astrup told Reuters, a decision that puts it at odds with NATO ally the United States. Nikolai Astrup, Norway's Minister of Digitalization, said that the Scandinavian nation does not ban suppliers.

Romania	<ul style="list-style-type: none"> Romania has set out the terms it will apply to choose a partner to implement 5G technology – which clearly excludes China's Huawei from the competition. The 5G tender in Romania has already been postponed three times and the current planned term is in the last quarter of 2020. 	<ul style="list-style-type: none"> August 2020: The Romanian government released a draft of legislation for public debate that will be used to determine which company carries out the installation of 5G networks in the country. China's Huawei looks unlikely to get the go-ahead as, according to the draft legislation, companies controlled by a foreign government, that don't have a transparent ownership structure, have a history of unethical corporate behaviour or are not subject to an independent justice system in their home country, are not eligible. 2019: memorandum of understanding between the governments of Romania and the US on 5G technology was signed in Washington. Romania was one of the first countries in the world to officially align with US opposition to involving Huawei in the upgrading of internet technologies.
Slovenia	<ul style="list-style-type: none"> August 2019: One national operator, Telekom Slovenia, announced a deal with Huawei's European competitor, Swedish firm Ericsson, on the eve of the state visit. Ericsson is supplying Telekom Slovenije with 5G technology for both the core and radio access networks, it said in a statement. Rollout actually began in late July, a week after the contract was signed, and the operator aims to increase 5G coverage to about a third of the Slovenian population, up from around a quarter today, said Ericsson. 	<ul style="list-style-type: none"> 2020: The Slovenian government pledged to scrutinize whether 5G vendors could be subject to influence from a foreign government, are transparent in their corporate structure, respect intellectual property rights and have a record of behaving ethically. 2020, August: The United States and Slovenia signed a deal Thursday to keep out "non-trusted" suppliers of 5G technology — the latest in a slew of agreements between Washington and some European capitals to elbow out Chinese telecoms giant Huawei.
Belgium	<ul style="list-style-type: none"> In June 2015 Proximus and Huawei signed a 5G MoU to bring 5G connectivity to two universities in Brussels. In November 2016 Proximus and Huawei successfully tested 5G technology. Telecom provider Proximus has launched its "5G light" network in 30 municipalities of Belgium. However, the network will not cover Brussels, as it exceeds the Region's radiation standards. On July 17 the Belgian regulator BIPT offered temporary licences to Cegeka, Entropia, Orange, Proximus and Telenet in the 3600-3800 MHz frequency band. Although this is not a permanent solution, it does at least allow telecoms operators to deliver speed boosts along the lines as to what has been promised over the years. As a point of comparison, Proximus and its lightweight 5G connectivity could see a 30% speed upgrade. Also, it is mainly available in only Dutch speaking areas. 	<ul style="list-style-type: none"> From December 2018, Belgium's cybersecurity agency was reportedly considering a ban on Huawei. In April 2019 Belgium's center for cybersecurity has found no evidence that telecoms equipment supplied by Huawei Technology could be used for spying, according to Reuters. In July 2020, Federal Minister for Telecom Philippe de Backer announced that Huawei will not be banned from Belgium's 5G-networks The Belgian National Security Council has previously announced that 'high risk' telecom suppliers are excluded from the 'core' of the future 5G-networks in Belgium. In areas that are not the core of the network, these suppliers will be allowed to constitute a maximum of 35% of the network. The suppliers will also not be allowed to base themselves in certain 'sensitive' zones, such as in the vicinity of military compounds. Belgian operators have indicated that they hope that the government will not reconsider and become more strict in the future, as they have been working with Huawei technology for an extended period of time. However, French telecoms operator Orange may cut its use of Huawei's mobile gear in Belgium

France	<ul style="list-style-type: none"> • The first full-scale 5G deployment tests began in January 2018 in several pilot cities in France with operators Orange, Bouygues Telecom, Free and SFR. • French telecom regulator Arcep announced that France's four mobile network operators – Bouygues Telecom, Free Mobile, Orange and SFR – had qualified to participate in the 3.4 – 3.8 GHz band frequency awards, planned for between 20 and 30 September. • Should the auction take place in September, Arcep said the licenses would then be awarded in October or November, allowing the operators to start their 5G service rollouts. • The regulator said it is removing the obligation for each operator to deploy 5G services in at least two cities before the end of 2020. • By 2030 5G should be available in the whole country. 	<ul style="list-style-type: none"> • In 2017, Orange and Huawei signed a partnership agreement to cooperate on 5G and cloudification technologies. • In December 2018, French Finance Minister Bruno Le Maire said Chinese tech giant Huawei was welcome in France, though the government could block certain investments. • France is listed among the countries who support the US Department of State initiative "The Clean Network" • Nevertheless, France will not be excluding any company including China's Huawei from its next-generation 5G mobile market, according to Reuters. • But, according to the earlier information, "French authorities have told telecoms operators planning to buy Huawei 5G equipment that they won't be able to renew licences for the gear once they expire, effectively phasing the Chinese firm out of mobile networks". Thus, companies not currently using the Chinese company's gear are encouraged to avoid switching to it. These restrictions would "de facto phase-out Huawei within France's 5G networks by 2028". • Orange have already said they will not use Huawei for their 5G equipment, choosing Nokia and Ericsson instead.
Albania	<ul style="list-style-type: none"> • According to the National Plan for Sustainable Development of Digital Infrastructure, Broadband 2020-2025 (approved 3.6.2020): "5G should be regarded as a key component of the Albanian Digital Society [...]. Hence, to achieve the goals of 5G service provision in 2021 as set out in the 5G Strategy, the 3.5 GHz band should be auctioned as soon as possible during 2020 and be a key part of the National Broadband Plan." • By the end of 2025, Albania plans to have a major city, the major transport corridors and strategic locations to be covered with 5G connectivity. • The national 5G strategy and roadmap are being finalized. 	<ul style="list-style-type: none"> • On August 12, Albania joined the US Department of State initiative "The Clean Network" • The 5G Clean Path is described as an "end-to-end communication path that doesn't use any transmission, control, computing, or storage equipment" from any of these companies. • Albania will not utilize any 5G services from "untrusted IT vendors" including Huawei and ZTE. • Official legal security regulations are still being finalized.

UK	<ul style="list-style-type: none"> • Britain's relationship with the U.S. is shaping its policy on 5G security. That includes calls for a hard reboot of its approach to China. • Partial market access into future telecoms networks for Huawei is allowed, but limited. • 2019: The operator O2, which is owned by telecom giant Telefónica, told the BBC in July it would roll out 5G without using Huawei equipment, instead opting for Ericsson and Nokia. • 2018: British Telecom has confirmed it is removing Huawei equipment from key areas of its 4G network after concerns were raised about the Chinese firm's presence in critical telecoms infrastructure • July 2020: Huawei to be removed from UK 5G networks by 2027. The decision follows a technical review by the National Cyber Security Centre in response to US sanctions. • 2020 British PM at the end of January announced the government will allow Huawei to sell equipment for 5G networks but keep its access limited to peripheral, non-sensitive parts of the network. It also imposed a cap of 35 percent on Huawei's market share — a type of measure that, so far, no European government has copied. • 2020: Parker, Britain's top security official, told ahead of the Americans' visit that he has "no reason to think" the U.K.'s intelligence sharing with the U.S. would suffer if it allowed Huawei market access • The UK Huawei Cyber Security Evaluation Centre (HCSEC), set up in 2010 to evaluate Huawei hardware and software, is controlled by the UK cybersecurity authority NCSC (part of the UK intelligence and security agency GCHQ). Its Oversight Board produces regular reports of its findings. • 2019: The UK NCSC notes that it still has strict controls for how Huawei is deployed – its technology is not accepted into sensitive networks, including those of the government • 2019: The NSCS said its inspections of Huawei's equipment were "arguably the toughest and most rigorous oversight regime in the world for Huawei," and the risk it posed was manageable, in a landmark speech by Executive Director Ciaran Martin in Brussels last year. • A top cyber-security official has said Huawei's "shoddy" engineering practices mean its mobile network equipment could be banned from Westminster and other sensitive parts of the UK. • 2018: The British security services' annual reviews also forced Huawei to pledge a \$2 billion investment to fix their software issues.
----	---

US	<ul style="list-style-type: none"> • White House flagged Huawei as a national security threat because of concerns the company could be used by the Chinese government for acts like cyberespionage. • Banned in general (some changes discussed below might slightly alter the current restrictions). • May, 2019: The Commerce Department separately adds Huawei to the Entity List, barring U.S. firms from selling or transferring U.S. technology to the company without a special license. U.S. President Donald Trump signs executive order empowering the Commerce Department to prohibit U.S. firms from purchasing foreign-manufactured telecommunications equipment. • July, 2020: U.S. Secretary of State Mike Pompeo announces U.S. visa restrictions on employees of Chinese technology companies, restrictions that will likely affect some Huawei employees. • June, 2020: The Federal Communications Commission announces its determination that Huawei and ZTE pose “a national security threat to the integrity of communications networks” and related supply chains. • May, 2020: The Commerce Department announces a revised rule that will expand U.S. authority to use licensing restrictions to constrain Huawei and affiliated companies from purchasing semiconductors made with U.S. technology in third countries. • June 2020: The United States on Monday confirmed a Reuters report that it will amend its prohibitions on U.S. companies doing business with China’s Huawei to allow them to work together on setting standards for next-generation 5G networks. • The move is significant because it means American firms will be able to have a seat at the table in the formation on so-called standards, which are specification and rules that govern how critical technologies work. • Last year, the United States placed Huawei on the Commerce Department’s so-called entity list, which restricted sales of U.S. goods and technology to the company, citing national security. • The United States adopted a law in 2018 prohibiting the purchase and use of telecommunications and surveillance products by specific Chinese companies. • The U.S. campaign pushing allied countries to cut ties with Huawei (e.g. signing some joint agreements • These are nonbinding, political pledges that, if implemented, would cut market access to suppliers that are subject to foreign interference, lack transparent corporate ownership structures and violate international ethical norms and intellectual property protections. • These agreements have little value if they are not backed up by law forcing telecoms companies to abide by their terms. • No incentives from the side of the U.S.. Washington secured the support of Romania, Poland, Estonia, Latvia and the Czech Republic, all of which have signed joint statements or memorandums with the U.S. government on 5G security.)
----	---