

SUPPORTING FREEDOM AROUND THE WORLD



NATIONAL  
ENDOWMENT  
FOR  
DEMOCRACY



# THE SECURITY RISKS CARRIED BY THE CHINESE TECH FRONTRUNNER HUAWEI



# The security risks carried by the Chinese tech frontrunner Huawei

Civic IDEA presents the second brief related to  
the security risks from the PRC,  
mainly referring to the Chinese tech giant "Huawei",  
its activities, and misdemeanors in Georgia and worldwide.

**SINCE 2019, HUAWEI HAS TAKEN AN HONORABLE PLACE AMONG OTHER CHINESE TECH COMPANIES  
IN THE US BANNED COMPANY LIST.**

Control Policy: End-User and End-Use Based

Supplement No. 4 to Part 744

ENTITY	LICENSE REQUIREMENT	LICENSE REVIEW POLICY
Huawei Technical Service Co., Ltd., China.	For all items subject to the EAR, see §§ 736.2(b)(3)(vi) <sup>1</sup> , and 744.11 of the EAR, EXCEPT <sup>2</sup> for technology subject to the EAR that is designated as EAR99, or controlled on the Commerce Control List for anti-terrorism reasons only, when released to members of a “standards organization” (see §772.1) for the purpose of contributing to the revision or development of a “standard” (see §772.1).	Presumption of denial.
<p>Huawei Technologies Co., Ltd., a.k.a., the following two aliases,                      -Shenzhen Huawei Technologies; <i>and</i>                      -Huawei Technology, and to include the following addresses and the following 22 affiliated entities:</p> <p>Addresses for Huawei Technologies Co., Ltd.: Bantian Huawei Base, Longgang District, Shenzhen, 518129, China; <i>and</i> No. 1899 Xi Yuan Road, High-Tech West District, Chengdu, 611731; <i>and</i> C1, Wuhan Future City, No. 999 Gaoxin Ave., Wuhan, Hebei Province; <i>and</i> Banxuegang Industrial Park, Buji Longgang, Shenzhen, Guangdong, 518129, China; <i>and</i> R&amp;D Center, No. 2222, Golden Bridge Road, Pu Dong District, Shanghai, China; <i>and</i> Zone G, Huawei Base, Bantian, Longgang District, Shenzhen, China.</p> <p>Affiliated entities:</p> <p><u>Beijing Huawei Longshine Information Technology Co., Ltd.</u>, a.k.a., the following one alias:                      -Beijing Huawei Longshine, to include the following subordinate.                      Q80-3-25R, 3rd Floor, No. 3, Shangdi Information Road, Haidian District, Beijing, China.</p> <p><u>Hangzhou New Longshine Information Technology Co., Ltd.</u>,                      Room 605, No. 21, Xinba, Xiachang District, Hangzhou, China.</p> <p><u>Hangzhou Huawei Communication Technology Co., Ltd.</u>,                      Building 1, No. 410, Jianghong Road, Changhe Street, Binjiang District, Hangzhou, Zhejiang, China.</p> <p><u>Hangzhou Huawei Enterprises</u>,                      No. 410 Jianghong Road, Building 1, Hangzhou, China.</p> <p><u>Huawei Digital Technologies (Suzhou) Co., Ltd.</u>,                      No. 328 XINHU STREET, Building A3, Suzhou (Huawei R&amp;D Center, Building A3, Creative Industrial Park, No. 328, Xinghu Street, Suzhou), Suzhou, Jiangsu, China.</p> <p><u>Huawei Marine Networks Co., Ltd.</u>, a.k.a., the following four aliases:                      -Huawei Marine;                      -HMN Technologies;                      -Huahai Zhihui Technology Co., Ltd.; <i>and</i>                      -HMN Tech.                      Building R4, No. 2 City Avenue, Songsan Lake Science &amp; Tech Industry Park, Dongguan, 523808, <i>and</i> No. 62, Second Ave., 5/F-6/F, TEDA, MSD-B2 Area, Tianjin Economic and Technological Development Zone,</p>	For all items subject to the EAR, see §§ 736.2(b)(3)(vi) <sup>1</sup> , and 744.11 of the EAR, EXCEPT <sup>2</sup> for technology subject to the EAR that is designated as EAR99, or controlled on the Commerce Control List for anti-terrorism reasons only, when released to members of a “standards organization” (see §772.1) for the purpose of contributing to the revision or development of a “standard” (see §772.1).	Presumption of denial.

Control Policy: End-User and End-Use Based

Supplement No. 4 to Part 744

ENTITY	LICENSE REQUIREMENT	LICENSE REVIEW POLICY
<p>Tianjin, 300457, China.</p> <p><u>Huawei Mobile Technology Ltd.</u>,                      Huawei Base, Building 2, District B, Shenzhen, China.</p> <p><u>Huawei Tech. Investment Co.</u>,                      U1 Building, No. 1899 Xiyuan Avenue, West Gaoxin District, Chengdu City, 611731, China.</p> <p><u>Huawei Technology Co., Ltd. Chengdu Research Institute</u>,                      No. 1899, Xiyuan Ave., Hi-Tech Western District, Chengdu, Sichuan Province, 610041, China.</p> <p><u>Huawei Technology Co., Ltd. Hangzhou Research Institute</u>,                      No. 410, Jianghong Rd., Building 4, Changhe St., Binjiang District, Hangzhou, Zhejiang Province, 310007, China.</p> <p><u>Huawei Technologies Co., Ltd. Beijing Research Institute</u>,                      No. 3, Xinxi Rd., Huawei Building, ShangDi Information Industrial Base, Haidian District, Beijing, 100095, China; <i>and</i> No. 18, Muhe Rd., Building 1-4, Haidian District, Beijing, China.</p> <p><u>Huawei Technologies Co., Ltd. Material Characterization Lab</u>,                      Huawei Base, Bantian, Shenzhen 518129, China.</p> <p><u>Huawei Technologies Co., Ltd. Xi'an Research Institute</u>,                      National Development Bank Building (Zhicheng Building), No. 2, Gaoxin 1st Road, Xi'an High-tech Zone, Xi'an, China.</p> <p><u>Huawei Terminal (Shenzhen) Co., Ltd.</u>,                      Huawei Base, B1, Shenzhen, China.</p> <p><u>Nanchang Huawei Communication Technology</u>,                      No. 188 Huoju Street, F10-11, Nanchang, China.</p> <p><u>Ningbo Huawei Computer &amp; Net Co., Ltd.</u>,                      No. 48 Daliang Street, Ningbo, China.</p> <p><u>Shanghai Huawei Technologies Co., Ltd.</u>,                      R&amp;D center, No. 2222, Golden Bridge Road, Pu Dong District, Shanghai, 286305 Shanghai, China, China.</p> <p><u>Shenzhen Huawei Antixin Electricity Co., Ltd.</u>, a.k.a., the following one alias:                      -Shenzhen Huawei Agisson Electric Co., Ltd.                      Building 2, Area B, Putian Huawei Base, Longgang District, Shenzhen, China; <i>and</i> Huawei Base, Building 2, District B, Shenzhen, China.</p> <p><u>Shenzhen Huawei New Technology Co., Ltd.</u>,                      Huawei Production Center, Gangtuo Village, Buji Town, Longgang District, Shenzhen, China.</p> <p><u>Shenzhen Huawei Technology Service</u>,                      Huawei Base, Building 2, District B, Shenzhen, China.</p> <p><u>Shenzhen Huawei Technologies Software</u>,                      Huawei Base, Building 2, District B, Shenzhen, China.</p> <p><u>Zhejiang Huawei Communications Technology Co., Ltd.</u>,                      No. 360 Jiangshu Road, Building 5, Hangzhou, Zhejiang,</p>		

Already in the [updated version of the list](#), which dates back to December 2021, we see that Georgia's leading strategic partner, the United States, has blacklisted not only the Huawei divisions in different cities in China but also its other branches abroad. More precisely, the US has barred exports, reexports, and transfers coming from the Huawei subdivisions in Argentina, Australia, Bahrain, Belarus, Belgium, Bolivia, Brazil, Burma, Canada, Chile, Costa Rica, Cuba, Denmark, Egypt, France, Germany, India, Indonesia, Italy, Jamaica, Japan, Jordan, Kazakhstan, Lebanon, Madagascar, Mexico, Morocco, Netherlands, New Zealand, Oman, Pakistan, Panama, Paraguay, Peru, Portugal, Qatar, Romania, Russia, Singapore, South Africa, Sweden, Switzerland, Thailand, Turkey, UAE, UK, Vietnam. According to the document, the main reason for their debarment is linked to the security vulnerabilities that Huawei items convey.

The alarm raised by the US is not at all groundless. The liabilities are also evidenced by the latest scandalous experience in the Netherlands. According to Dutch news, from April 2021, a leaked internal report by the most prominent national telecom provider, KPN, acknowledged that Huawei, its leading equipment supplier since 2009, has been improperly [monitoring](#) the calls of 6.5 million users without the KPN knowing. The [confidential report](#) completed by the tech consultancy firm *Capgemini* revealed that Huawei representatives in the Netherlands and China could surveil the conversations that then PM Jan Peter Balkenende might have conducted. The calls made by the Chinese dissidents might have also been recorded.

*"The continued existence of KPN Mobile is in serious jeopardy as licenses can be revoked or government and businesses can relinquish their trust in KPN if it is known that the Chinese government can eavesdrop on KPN mobile numbers and shut down the network,"* the [report](#) said.

While such scandals are disclosed to the public, we obviously start wondering about the origins of this company. Huawei was founded in 1987 by [Ren Zhengfei, a former member of the Chinese People's Liberation Army \(PLA\)](#). Huawei is claimed to be a private company responsible for delivering ["information and communications technology \(ICT\) infrastructure and smart devices."](#) Gradually, Huawei established itself as [the largest seller](#) of telecommunications hardware and 4G/5G networks and currently operates in 170 countries, including Georgia.

Huawei has been involved in numerous scandals, and its officials have been under scrutiny and imprisoned several times for alleged fraud and other corruption activities [in different parts of the world](#). The latest arrest happened in 2018 when Huawei chief financial officer (CFO) Meng Wanzhou was detained and taken into custody by the Canadian police in Vancouver due to the US accusations of fraud committed by her ["by lying to American banks about her company's ties to a telecommunications firm that did business in Iran."](#)

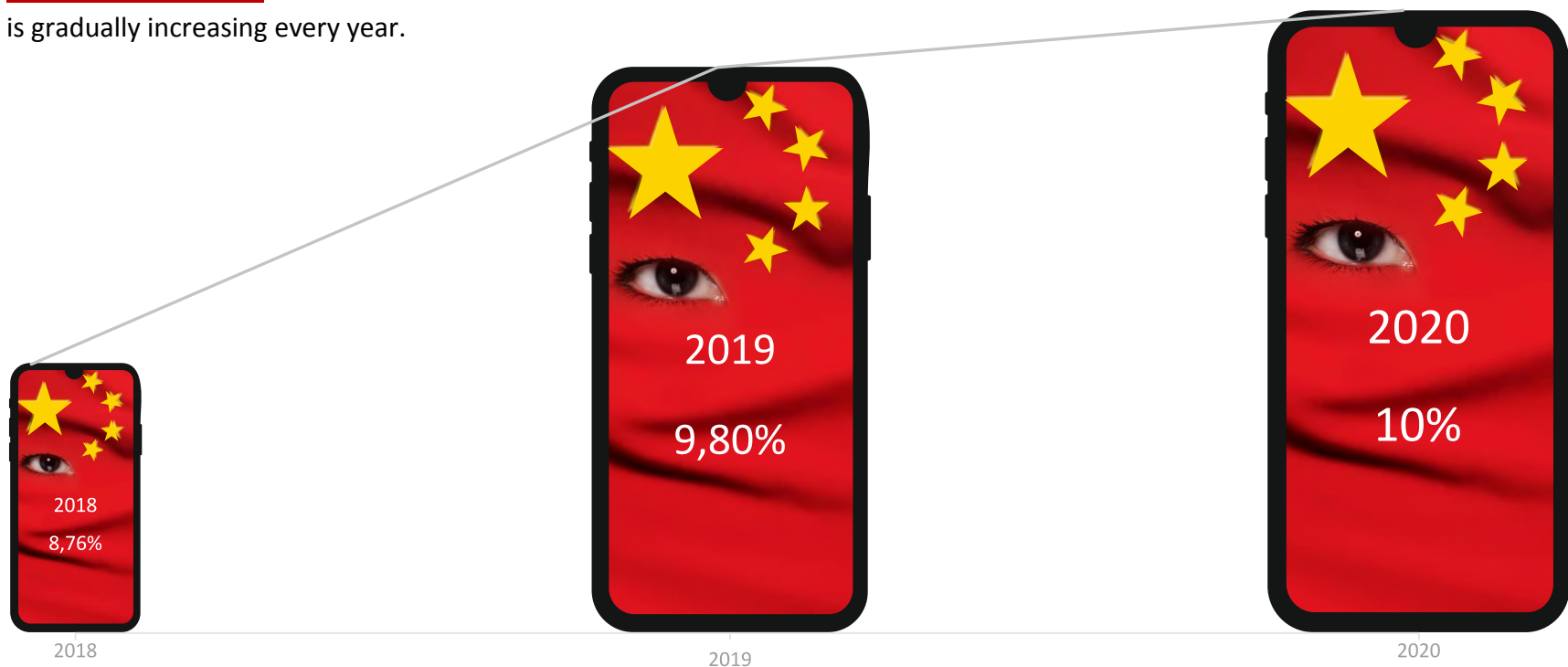
Huawei has been operating in Georgia for more than 20 years. It first appeared [on the Georgian market in 2001](#), and until May 2008, [Huawei's foreign branch](#) "Huawei Tech. Invest-

ment Co. Limited” partnered with local ISPs and operators to build communications and mobile networks. In May 2008, Huawei officially registered a branch in Tbilisi, „Huawei Technologies Co. Ltd“. From 2013, the Chinese tech giant started selling smartphones. Huawei has been very successful in Georgia because Georgian telecommunications companies are actively cooperating with it, along with its other Chinese counterparts, such as ZTE, Hikvision, Dahua, and Hytera. However, a large portion of its sales still come from smartphones and hardware devices. It should be noted that in 2018, Huawei occupied 8.76% of the Georgian market; in 2019, it accounted for 9.8% of sales of new smartphones, and in 2020, its sales grew to 10%. This occasion shows us that its influence is gradually increasing every year.



## Distribution of smartphones by Huawei in Georgia

—— Sales





In 2020, the US Embassy in Tbilisi announced reducing cooperation with Georgian companies that use Huawei technologies. Huawei has been actively partnering with the company “Silknet”, a leader in providing telecommunications services to the Georgian population and a wide range of organizations, for years. The Chinese company is responsible for providing hardware, software, and services related to them. Moreover, in 2019, “Silknet”, in partnership with Huawei, introduced the “Gigabit LTE” internet in the Western part of Georgia. According to the Georgian brand of Radio Free

Europe/Radio Liberty, the Chinese company's equipment is also used by government agencies. For example, 200 Huawei tablets are used by Georgian MPs. In 2015, Georgian Prime Minister officially met with the senior Vice President of Huawei, Tsu Wenchu. The meeting revealed that Huawei aimed to assist the Georgian government in implementing the e-government project initiated by the Georgian PM. Huawei has also expressed interest in the concept of a so-called "safe country", which involves the installation and insurance of security systems in Georgian cities and regions.



(Source:  
<https://www.facebook.com/media/set/?set=a.915750151849395.107374350.1.373058439451905&type=1>)

Civic IDEA requested information from the Administration of the Government of Georgia on how the collaboration between the two parties developed in the following years. The government surprisingly forwarded our letter to the Ministry of Economy, which itself answered that has no information concerning the "safe country" concept and other issues raised during the meeting between the Prime Minister of Georgia and the representatives of Huawei.

Nevertheless, not all Georgian public institutions and companies are open about their partnership with Huawei. On the website of the leading telecommunication operator in Georgia, "Magti", we can only find one article about [Huawei's involvement in developing a 4,5G network](#). The Georgian company refuses to give details about its close collaboration with the Tech giant. Overall, the information about the contracts, MOUs, and other types of cooperation established between the Chinese tech giant and the Georgian state or private entities is not transparent.

In our 2020 report ["Who is in charge of the post-cold war world? Chinese influence operations in Academia, Media & CSOs,"](#) we have thoroughly covered the controversies related to Huawei and its activities in the US, the UK, and different EU member states. We also reviewed the resilience strategies used by multiple countries, such as Japan, the US, or the UK, that effectively impose restrictions and sanctions against the Chinese tech giant to ensure their national security. Although Huawei is considered a private company, it and its sister technology giants are easily influenced by the Chinese

Communist Party and effectively pursue their policies in China and worldwide. Accordingly, Huawei is effectively using technological devices to [provide intelligence and critical data to the Chinese government](#), directly threatening the national security of various states. Therefore, we can conclude that the problem related to Huawei is less technical and more associated with political and geopolitical challenges.

In our report, we wanted to present in detail the national security risks and scandalous cases associated with Huawei's activities around the world. In addition, we would like to urge the Georgian government and private companies to be more transparent about their cooperation with the Chinese tech frontrunner and, before concluding new contracts, to take into account the high-security risks associated with Huawei that have been revealed through the controversial experiences and the warnings of Georgia's strategic partners.