

# MP-IDSA

## *Issue Brief*

# US Tech Sanctions on China

*Halima Z. Ansari*

July 13, 2022

## **S***ummary*

China's technology sector has faced challenges due to sanctions imposed by the United States. The acceleration of tech sanctions by the US, on account of the role these companies are playing in aiding Chinese governmental repressive activities in places like Xinjiang, coincides with the rise of China's Digital Silk Road (DSR) enterprise under the Belt and Road Initiative. Chinese tech companies, on their part, are making efforts to ensure self-sufficiency in the manufacturing and production of crucial technologies, supported by government policies focused on the science and technology sector.

## Overview

In the last five years, China’s technology sector has faced challenges due to sanctions imposed by the United States.<sup>1</sup> Reports in May 2022 noted that the Biden Administration was contemplating placing Hikvision, a Chinese security equipment maker, on the US’s Specially Designated Nationals (SDN) list.<sup>2</sup> Hikvision has been previously blacklisted by the White House in 2021 due to apprehensions about the use of the company’s security equipment in Xinjiang, contributing to human rights abuses on Uyghurs. The company’s relationship with Beijing and the People’s Liberation Army (PLA) have also raised concerns.

The acceleration in tech sanctions by the US coincides with the rise of China’s Digital Silk Road (DSR) enterprise under the Belt and Road Initiative (BRI). Public–Private partnership in critical information infrastructure is a characteristic feature of the DSR. Hikvision, like many private Chinese companies, has collaborated with Beijing on several of DSR’s undertakings, particularly in Africa. Sanctions by the US, thus, impact these BRI projects.

## US Sanctions on Huawei and Hikvision

The Digital Silk Road has shifted the world’s attention from BRI’s hard infrastructure projects to its softer information and technology-related projects. After Donald Trump took office, several policy measures were taken targeting Chinese science and technology policies. These include the National Defence Authorization Act 2019, Uyghur Human Rights Policy Act 2020, and the Hong Kong Autonomy Act 2020, which have imposed sanctions on China-based entities.

In May 2019, Huawei, the Chinese tech company, was subjected to some of the biggest sanctions in the tech industry. The company was added to the Commerce Department’s Entity List, leading to stricter export controls.<sup>3</sup> Shortly after, it was unable to do business with any organisation that was based in the US. Previously, in August 2018, Australia had also banned Huawei from supplying equipment for its 5G mobile network, citing security concerns.<sup>4</sup> By 2020, Huawei was unable to work with companies such as Google and Intel. Since Huawei smartphones could no longer support Google-owned applications, it suffered huge losses in its sales outside China.

The Biden administration has not departed from Trump-era sanctions. In May 2022, reports of US plans to put Hikvision on its SDN List, in adherence to the Global Magnitsky Act 2016<sup>5</sup>, emerged.<sup>6</sup> The SDN list usually contains entities such as

---

<sup>1</sup> See Executive Order 13959 of November 12, 2020; Executive Order 13818 of December 20, 2017; Supplement No. 4 to Part 744 - ENTITY LIST.

<sup>2</sup> Demetri Sevastopulo, [“US Moves towards Imposing Sanctions on Chinese Tech Group Hikvision”](#), *Financial Times*, 3 May 2022.

<sup>3</sup> [“Entity List”](#), Bureau of Industry and Security, U.S. Department of Commerce.

<sup>4</sup> [“Huawei and ZTE Handed 5G Network Ban in Australia”](#), *BBC News*, 23 August 2018.

<sup>5</sup> The Global Magnitsky Act authorises the US Government to sanction foreign entities on grounds of human rights abuse. See [Global Magnitsky Human Rights Accountability Act](#).

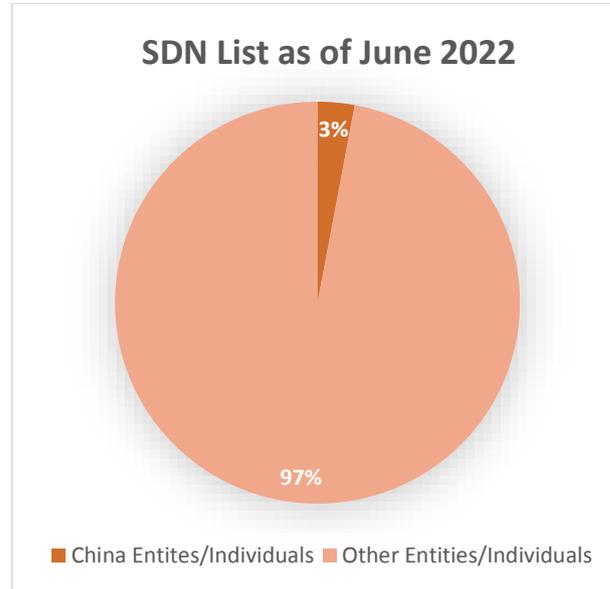
<sup>6</sup> Demetri Sevastopulo, no. 2.

terrorists or narcotics traffickers and very few firms of Hikvision’s scale find a mention in the list. SDN is one of the highest degrees of sanctions imposed by the US—the assets of any entity on the list are blocked, and US persons are prohibited from dealing with them.

Hikvision has been subjected to sanctions by the US in previous years as well. In June 2021, Biden signed an executive order to prohibit US investments in Chinese surveillance technology companies that “facilitate serious human rights abuses” or “undermine the security or democratic values of the United States”, adding 59 entities to its new Chinese Military-Industrial Complex Companies List which included Hikvision.<sup>7</sup> Hikvision was prohibited from importing US-origin goods without a license or selling products to US federal agencies.

While Huawei’s violation of US sanctions against Iran was cited as the immediate cause behind its sanctioning, along with concerns related to cybersecurity, Hikvision’s relationship with the PLA and the alleged supply of its products to camps in Xinjiang was listed as the primary cause behind the current sanctions.

A self-described leader in AIoT (Artificial Intelligence of Things), Hikvision manufactures and sells fingerprint terminals, face recognition terminals, video intercoms, thermal cameras, checkpoint radars, surveillance cameras, among other equipment. Although Hikvision has released several ‘white papers’ on cybersecurity and its commitment to the GDPR compliance<sup>8</sup>, Washington’s apprehensions about the company have not been quelled.<sup>9</sup>

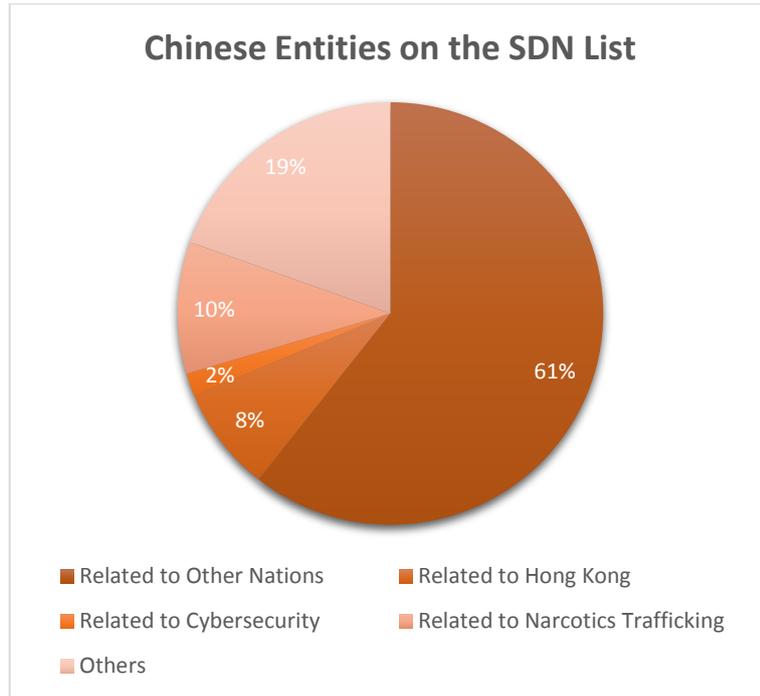


---

<sup>7</sup> [“Fact Sheet: Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People’s Republic of China”](#), The White House, 3 June 2021.

<sup>8</sup> The General Data Protection Regulation (GDPR), entered into force in 2016, after being passed by the European Parliament. It levies data privacy and security standards on any organisation that collects data related to the European Union.

<sup>9</sup> [“Hikvision Cybersecurity White Paper 2019”](#), Hikvision.



**Source:** U.S Department of The Treasury<sup>10</sup>

Hikvision in its response to the SDN placement has stated that “any such sanction should be based on credible evidence and due process”.<sup>11</sup>

## The Digital Silk Road

To understand the relationship between US sanctions and China’s DSR, it is important to survey the role private Chinese companies have played in the establishment of the latter. Companies like Huawei, Alibaba, Tencent, Baidu, Hikvision and ZTE, amongst others, are the main drivers of the DSR.<sup>12</sup> During the second Belt and Road Forum in 2019, a separate forum was dedicated to the DSR, where close to 15 companies signed new projects with various governments.<sup>13</sup>

Huawei, for example, has played a significant role in setting technology standards for 5G in many BRI countries. It has signed deals with several African and Latin American countries for projects related to 5G, smart city, and fibre-optic cables under the umbrella of the DSR. Heads of State of Sierra Leone and Uruguay have

<sup>10</sup> Available at [U.S Department of The Treasury](#) and [Office of Foreign Assets Control](#).

<sup>11</sup> [“US. Considers Imposing Sanctions on China's Hikvision”](#), *Reuters*, 4 May 2022.

<sup>12</sup> Chinese entities have provided more than US\$ 17 billion to various DSR undertakings. The DSR has also been promoted widely by Beijing through the Second Belt and Road Forum (BRF) and the 5th World Internet Conference (WIC) and includes projects on trans-oceanic fibre-optical cables, smart cities, cross-border e-commerce, artificial intelligence, big data and quantum computing.

<sup>13</sup> [“List of Deliverables of the Second Belt and Road Forum for International Cooperation”](#), The Second Belt and Road Forum for International Cooperation, 27 April 2019.

also visited Huawei headquarters in China. In 2019, Sierra Leone signed a US\$ 30 million loan agreement with the Export-Import Bank of China to finance Huawei’s construction of the second phase of its national fibre-optic project.<sup>14</sup> In the same year, Huawei also signed an agreement with Kenya for a US\$ 173 million smart city project in Konza Technopolis.<sup>15</sup> A MoU with Uruguay was signed for the development of 5G network, ICT training and industrial digitisation.<sup>16</sup>

Like Huawei, Hikvision is also integrated with several DSR projects, although many of the details of these projects have not been released publicly. Hikvision has an important project in Zimbabwe, in close collaboration with CloudWalk Technology, an AI company that makes facial recognition software.<sup>17</sup> *ChinAfrica* reports that Hikvision is also working on Zimbabwe’s pilot smart city project in Mutare.<sup>18</sup> Together, Hikvision and another Chinese company, Dahua, also supply nearly 40 per cent of the world’s surveillance cameras.

## US Concerns

Rising competition in the international tech market, and Chinese influence on technology standardisations and cyberspace norms have been some of the primary concerns of Washington. BRI’s Digital Silk Road, not only facilitates export of Chinese technology to previously untapped markets, but also gives an opportunity to private Chinese firms to expand extensively. This enables Beijing to inflate its influence on the international tech sector, which has been dominated by the West since its inception. Companies like Huawei, Hikvision and ZTE have already taken major business away from Western companies like IBM and Cisco.

These and other concerns were voiced at a US House of Representatives meeting on ‘China’s Digital Authoritarianism’ in 2019. It was highlighted that an increase in Chinese tech exports was bound to give developing and underdeveloped countries ‘the technological tools they need to emulate Beijing’s model of social and political control’.<sup>19</sup>

Several policy documents from the White House detail the dangers of exporting a ‘Chinese model of surveillance state’ onto the rest of the world. The addition of smart city projects, like the ones undertaken by Hikvision, has garnered attention from policy-makers in the US. Smart Cities are municipalities that use information and

---

<sup>14</sup> [“Huawei, Sierra Leone Deepen Partnership; Exim Bank to Fund Phase 2 of National Fiber Optic Backbone Project”](#), *Janes IntelTrak*, 5 September 2019.

<sup>15</sup> [“Huawei Deepens Cooperation with Botswana Police, Installing Cameras in Francistown”](#), *Janes IntelTrak*, 28 August 2019.

<sup>16</sup> [“Huawei to Build 5G Network in Uruguay”](#), *Janes IntelTrak*, 28 August 2019.

<sup>17</sup> [“Networking the ‘Belt and Road’ – The Future is Digital”](#), Mercator Institute for China Studies, 28 August 2019.

<sup>18</sup> Problem Masau, [“Face of the Future”](#), *ChinAfrica*, 10 August 2018.

<sup>19</sup> [“Chinas Digital Authoritarianism: Surveillance, Influence, and Political Control \(Open\)”](#), U.S. House of Representatives, Permanent Select Committee on Intelligence, 16 May 2019.

communication technologies (ICTs) to automate their operations. About 114 smart city contracts involving Chinese vendors have been signed outside China since 2009.<sup>20</sup>

## Implications for Chinese Tech Companies

US sanctions on Chinese companies has resulted in complications in two main areas—market access and production. Exclusion from US technology will lead to issues in production. A prime example of this is Huawei, which struggled to create its Kirin chipset, produced by TSMC, which uses American technology, after the 2019 blacklisting. Huawei reported having suffered US\$ 30 billion in annual losses following the sanction. Huawei’s revenues fell 29.4 per cent in the first half of 2021, from the previous year.

Although Huawei has a monopoly on 5G technology, rotating Chairman Eric Xu Zhijun, in a press briefing in 2021, stated that it would take Huawei many years before its 5G monopoly could compensate for these losses.<sup>21</sup> Since Huawei could not support Google-owned apps, its international smartphone market declined drastically. Exports fell and smartphone sales nearly halved to 134.7 billion yuan in 2020 from 255.8 billion yuan in 2019.

Hikvision, like Huawei, has a strong foothold in international markets and exports its products to 180 countries. *Financial Times* reports that the US administration has already started briefing Washington’s allies on the upcoming SDN sanction.<sup>22</sup> This means that governments that continue to deal with Hikvision would risk violating US sanctions, which may lead to Hikvision losing many of its international markets.

These implications may also lead to complexities in the DSR undertakings dependent on companies like Hikvision, especially in African and Latin American nations. As seen in the case of Huawei, any obstacle in logistics, supply chains, production or exports will have ramifications for the company’s operations. Since Hikvision’s sanctions measures will be on a much bigger scale than that targeted Huawei, these ramifications may multiply. Experts have opined that an SDN sanction on Hikvision might even lead to the demise of the company.<sup>23</sup> In that event, Hikvision’s DSR project in places like Zimbabwe might come to a standstill until alternative vendors are procured.

In addition, the sanctions on Hikvision risk creating a dangerous precedent for other Chinese tech actors integrated with the DSR, and which work on a global scale. US

---

<sup>20</sup> [“The Digital Silk Road: Expanding China’s Digital Footprint”](#), *Eurasia Group*, 8 April 2020.

<sup>21</sup> Che Pan, [“Huawei Says US Sanctions Cause US\\$ 30 billion Annual Loss in its Smartphone Business”](#), *South China Morning Post*, 24 September 2021.

<sup>22</sup> Demetri Sevastopulo, no. 2.

<sup>23</sup> [“US Tech War Targets Hikvision; China Wedges Australia on Solomon Islands”](#), *South China Morning Post*, 6 May 2022.

sanctions on Chinese companies, thus, have kept expansion of China’s influence in the tech sector in check, and have created hurdles for BRI’s DSR.

## China’s Shift to Technological Independence

When Huawei was initially added to the Entity List, the company responded by filing a lawsuit against the US Department of Commerce. However, little came of the legal battle that followed. Huawei soon shifted its focus and resources to navigating its operations around the ban and is now trying to function completely independent of all US-sourced technology, including Google. Its Harmony OS has been a quick replacement for Android and it is currently trying to attract developers to add their apps to its own version of an app store—the App Gallery.

Huawei’s efforts do indicate that sanctions by Washington are pushing Chinese companies to make efforts to ensure self-sufficiency in manufacturing and production of technologies. The Chinese economy, in previous decades, has been reliant on technological support from industrially developed nations. It was quickly realised by Beijing that this disables China from exiting the West’s monopoly over critical technologies.

US sanctions pressure is also in the context of China pursuing policies like Made in China 2025 (MIC 2025), which emphasises technological independence and self-reliance. Instituted in 2015, MIC 2025 aims to help China skip the middle-income trap by installing technology-powered production as opposed to labour-intensive production and ultimately aid in the development of an “Internet Superpower”. The 14<sup>th</sup> Five Year Plan, covering the years 2021 to 2025, also strongly emphasises the strategic importance of the development of science and technology and is further complemented by policies such as the Internet+ and the New Generation Artificial Intelligence Development Plan.<sup>24</sup>

In a direct response to Washington’s 2019 Entity List, China’s Ministry of Commerce, in the same year, also announced an ‘Unreliable Entity List’ regime, under which ‘punitive measures may be imposed on foreign entities for conduct that is contrary to China’s national interest or discriminatory against a Chinese enterprise’.<sup>25</sup> Although there were reports of companies like Apple and Cisco becoming the primary targets for the list, no updates have been disclosed since its release.<sup>26</sup> Beijing may respond with similar or more severe measures to Hikvision’s sanction.

---

<sup>24</sup> Internet+, proposed in 2015, aims to scale the usage of internet technology onto Chinese domestic industries like healthcare and education. The New Generation Artificial Intelligence Development Plan, released in 2017, charts the guidelines and principles of Artificial Intelligence development in China, providing recommendations and identifying potential challenges to the sector.

<sup>25</sup> [“MOFCOM Order No. 4 of 2020 on Provisions on the Unreliable Entity List”](#), Ministry of Commerce, People’s Republic of China.

<sup>26</sup> [“China Ready to Put Apple, Other U.S. Companies in 'Unreliable Entity List': Global Times”](#), Reuters, 15 May 2020

## **Conclusion**

Sanctions on a billion-dollar Chinese company like Hikvision will exacerbate the geopolitical rift between the US and China. This comes at a time when developments like the Russia–Ukraine crisis and the Covid-19 pandemic have added new and delicate complexities to US–China geo-strategic competition. It is, thus, not surprising to note that China’s booming S&T sector is increasingly moving towards self-reliance and self-sufficiency in an attempt to curb future disruption that can be caused by US sanctions, especially on its DSR endeavours.

## About the Author

**Ms Halima Z. Ansari** is Research Intern at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

**Manohar Parrikar Institute for Defence Studies and Analyses** is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

*Disclaimer:* Views expressed in Manohar Parrikar IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the Manohar Parrikar IDSA or the Government of India.

© Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA) 2022