

*INSS Insight* No. 1193, July 15, 2019

**My Way or the Huawei?**

**The United States-China Race for 5G Dominance**

**Hiddai Segev, Doron Ella, and Assaf Orion**

**The race for dominance in the data highways of the future is at the forefront of the strategic competition between the United States and China. The two powers compete for other countries' support and infrastructure, seeking to obtain technological, economic, and security advantages. Banning Chinese companies from fifth generation infrastructure (5G) projects is the most explicit demand the United States administration has made of Israel, including clear linkage to American security assistance and intelligence cooperation. Thus, it is clear that Israel has but to comply with US demands on this issue, while at the same time continuing to develop its relations with China in fields where trade and investment activities do not entail serious risks to its own national security or to its vital strategic alliance with the US.**

In May 2019, the US Department of Commerce placed the Chinese telecommunications company Huawei on an "entity list" that prohibits American companies from supplying it with goods and services without special government approval. As a result, dozens of US and other companies such as Google, Vodafone, and Panasonic announced that they would freeze or limit their cooperation with the Chinese company and would cease selling it hardware and software. However, it was also reported that various American companies such as Intel and Micron continue to sell equipment to Huawei despite these restrictions, by marking their products as manufactured outside of the United States. On the sidelines of his meeting with Chinese President Xi Jinping at the G20 summit in late June 2019, President Trump announced that he would cancel the restriction, but added that there would be no exports of technology that posed a threat to United States national security. The United States is still clearly concerned about the economic and security risks of Huawei's global expansion, be it in the construction of 5G networks or in dominance of various communications markets.

These developments follow the measures taken by the administration against the Chinese company, led by federal legislation of August 2018 that prohibited use of Huawei products among administration employees. The principal US charge against Huawei appears in a Pentagon report of April 2019 on 5G infrastructures: "Evidence of backdoors or security vulnerabilities have been discovered in a variety of devices globally. Many of

these seem to be related to requirements from the Chinese intelligence community pressuring companies to exfiltrate information about domestic users” The report also points to the Chinese Cyber Law of June 2017, which conditions the continued operation of foreign companies in China on their relaying information and technologies to Chinese authorities, if necessary. It was later reported that the United States has proof that Huawei receives funding from the Chinese security establishment; China has denied these allegations.

The US measures against Huawei stem from both “classical” national security and mid to long term economic competition concerns. The United States views the preservation of its technological superiority in the world as a primary interest that flows into all dimensions of its national power: military, economic, scientific, and political. China, as an emerging economic and technological power, is seen as a major threat, especially in view of its advanced capabilities in developing and deploying 5G infrastructure through its communications companies, some of whose products are more advanced than those currently possessed by the United States. Thus, the United States views China as a direct threat to its technological and economic supremacy, and accordingly strives to delay and even prevent China’s becoming a global leader in technologies that the United States considers to be strategic.

That said, American pressure on its allies to ban Chinese involvement in the construction of communications infrastructure seems to be related also to traditional security considerations. According to senior US officials, Huawei's cooperation with various countries jeopardizes their intelligence and security cooperation with the United States, as it allows a possible loophole for Chinese access to US infrastructure and secrets. For example, the United States warned South Korea that if it installed Huawei's 5G infrastructure, the US would not be able to share intelligence and provide it with security assistance vis-à-vis North Korea. A similar warning was sent to Germany and to other governments.

Members of the Five Eyes intelligence alliance have yet to formulate a unified risk management policy on the subject. While the United States and Australia have decided to ban the entry of Chinese communications infrastructures (as well as Japan and other non-Five Eyes members), Canada and New Zealand have yet to decide, and reports suggest the United Kingdom has allowed the entry of Chinese communications infrastructure, but without core technologies. The contrasting approaches adopted by United States partners reflect different equilibrium points between considerations of political independence, aspirations for economic relations with China, and recognition of the importance of their relations with the US government. The contrasting approaches also reflect different levels of Huawei involvement in each country, the differences in each country's threat

perception, and the economic, political, and security implications of Huawei's involvement. Despite US pressure, however, Huawei has gained more international commercial contracts for the supply of 5G infrastructure, and as of June 2019 signed 50 contracts in 30 countries.

The steps taken by the United States against Chinese communications companies in general and Huawei in particular point to a possible trend of American efforts to decouple advanced techno-economic fields, including 5G communications, into two global communications standards: one, led by Chinese giants, such as Huawei and ZTE, that are connected with the Communist Party and possibly the country's military; and another, Western-American, led by companies such as Nokia, Ericsson, and others, including in Asia. The competition between the two Great Powers to mobilize countries for each system is now in full swing. The emphasis by the US administration on 5G infrastructure deployment, especially among its close partners, points to the issue being at the forefront of the US-China Great Power competition, and at the heart of US interests.

US warnings about Chinese communications companies, especially about Huawei, have been conveyed to Israel explicitly by the highest echelons of the administration. On March 26, 2019, during Prime Minister Netanyahu's visit to the United States, President Trump reportedly warned that "If Huawei and ZTE establish a 5G communications network in Israel, security cooperation between the two countries might be limited, and security assistance reduced." Later reports claimed that National Security Advisor John Bolton likewise warned Israel not to allow the installation of Chinese cellular networks. US Undersecretary of Defense for Policy John Rood made similar remarks during a visit to Israel in early July.

In addition to a share of around 3.5 percent of the mobile device market in Israel, Huawei has a development center in the country operating under the name Toga Networks, and owns HexaTier, focusing on cyber security and database protection. Huawei has also invested in Elastifile, a cloud storage company, which was recently acquired by Google. It was recently reported that Huawei had opened a representative office in Israel to sell equipment and maintenance services to companies that build solar power facilities. According to several reports, this activity will enable it to gain access to data on the Israeli electricity sector and expand its hold on the sector.

### **Implications and Recommendations for Israel**

Between the two powers, the United States is Israel's strategic ally, and whereas China is an important trading partner. As with defense exports, when the United States defines a severe threat to its national security and to mutual security relations, Israel cannot ignore it. Steps taken by the United States directly against Huawei, and warnings by senior

administration officials against the company's involvement in Israel's communications infrastructure reflect the issue's position at the top of the administration's present agenda. The warning that was chosen by the United States, possible damage to the security aid, aims at a supreme Israeli interest and a main pillar of its national security.

The Huawei case is a relatively simple policy challenge for Israel, for two reasons. First, Israel and the United States have a wealth of experience and relatively broad common ground in cyber risks perceptions. Second is the high importance placed on the issue by the United States. Israeli media previously reported that "the State of Israel, through the National Authority for Data Protection at the Israel Security Agency (Shin Bet), does not allow China to build communications infrastructures of any kind in the country, and Israeli communications companies toe the line with the security authorities' position refraining from using Chinese components in their communications equipment." In light of all this, it is highly unlikely that Chinese components will be installed in Israel's fifth generation infrastructure.

Just as in the field of defense exports to China and the agreements Israel has with the United States, Israel should engage in a deep and ongoing dialogue with the administration, and maximize the deep cooperation between cyber agencies in order to manage the risk professionally and jointly. There is a need for Israel to deepen its understanding of US policy and its conduct on related issues, such as steps in US territory, US demands from its global partners, and their ways of dealing with the challenge. In light of the fact that the United States policy on this issue as well is a work in progress, there is a need to follow developments on an ongoing basis and to update Israel's policy accordingly.

Israel's dealings with China, should be respectful and practical, striving to attain China's understanding of its telecommunications policy, on similar lines to China's acceptance of Israel's "no defense exports" policy due to national security considerations. Insofar as this policy is accepted by the government of Israel, it should be expressed publicly and clearly both in Israel and abroad, in light of the considerable public diplomacy challenges that encircle the China-United States-Israel triangle.