Control of the Global Technology Market: The Battle of the Superpowers

Hiddai Segev and Galia Lavi

In early December 2018, Meng Wanzhou, CFO of Huawei and the daughter of the company's founder, was arrested in Canada at Vancouver Airport. The arrest was made at the request of the United States, for an alleged breach of American and European sanctions on Iran. While the Chinese government strongly condemned the arrest and demanded Meng's release, the incident highlighted the broader struggle between the United States and China for control of the global technology market and the future international standards in this field. Israel, which enjoys special strategic relations with the US and growing trade relations with China, must choose its moves wisely to avoid being caught in the inter-power struggle.

Keywords: China, United States, Huawei, communications, networks, 5G

In early December 2018, Meng Wanzhou, CFO of Huawei and the daughter of the company's founder, was arrested in Canada at Vancouver Airport. According to the indictment filed against her, in the years 2009-2014 Huawei operated in Iran through a subsidiary called Skycom. If Meng is found guilty of deceiving the banks regarding the link between the companies, she faces 30 years in prison. Although the arrest came immediately after the meeting of US President Donald Trump and Chinese President Xi Jinping at the G20 Summit in Buenos Aires, where the trade war crisis between the two powers was clearly on the agenda, there may not be a direct link between the two events. The Chinese government strongly condemned the arrest and demanded Meng's release, but the incident highlighted the broader struggle between the United States and China for control of the global technology market and the future international standards in this field.

Hiddai Segev is a research assistant at INSS. Galia Lavi is a research associate at INSS.

This article examines the essence of the struggle, presents the responses of various countries, and proposes recommendations for Israel. In order for Israel to protect its good relations with both the United States and China and avoid being injured in the crossfire, it must take three steps: maintain an ongoing dialogue with the United States and Western countries; define suitable review processes; and set up a mechanism for clear communication with China.

The Struggle for Future Global Control

The United States and China are struggling for control of the global technology market in general, and for the infrastructure for fifth generation (5G) networks in particular. These networks make it possible to transfer data at a speed of 1 gigabyte per second, ten times faster than today's 4G networks, and they enable advanced technologies such as artificial intelligence (AI), the internet of things (IoT), and big data to work much faster. Control of communications networks is a strategic asset that affects governments, technology companies, industries, and people, since it allows control of the flow of information and governs how it is stored and utilized for commercial, security, and strategic needs. Therefore, both the United States and China have an interest in determining international standards in the field and thereby control future access to the networks.

The United States is working energetically to be the leader in this technology race. Its national defense strategy for 2018 explicitly states that it seeks to promote big data and AI technologies, in order to have an advantage over its rivals. In October 2018, President Trump signed a presidential memorandum with instructions for long term national strategic planning on this issue, and announced the formation of a team in the White House to guide federal authorities, in conjunction with the private sector, on the utilization of 5G networks. At the same time, leading internet providers in the United States such as Verizon, AT&T, and T-Mobile began to examine the use of 5G networks.[1]

China too considers anything relating to 5G as supremely important, and it has often declared its wish to be a world leader in the new networks in accordance with its national vision of Made in China 2025; the goal is to promote its industry and economy and make China independent in the development and manufacture of advanced technologies. Already in 2012, two years before the entry of 4G technologies to the country, several Chinese companies embarked on a joint effort to conduct research and

development of the 5G technologies expected to be in commercial use by 2020. In addition, and like the United States, China is already working on the development of sixth generation (6G) communications networks – which will enable data transfer of 1 terabyte per second, and which are expected to be ready by 2030.[2]

The chokepoint that worries the United States in particular is the fact that there are currently only four companies in the world engaged in building 5G networks. Two are Chinese – Huawei and ZTE, and two are European – Erikson and Nokia. The Korean company Samsung has also recently taken steps to enter this market, but it has little experience. The surprising absence of the United States from this field may perhaps be explained by the assumption that control of chips, essential for the 5G networks through the monopolies of Qualcomm and Intel (both American companies), will be sufficient to ensure control of the entire field.

Huawei Technologies Co., Ltd. is a private company that was established in 1987 by Ren Zhengfei, a former engineer in the Chinese army. The company, headquartered in Shenzhen in southern China, employs about 180,000 people. As of 2017, Huawei was considered one of the world's largest providers of communications with revenues of about $92 billion – largely from overseas transactions. In 2018, the company supplied some 10,000 5G communications stations to various countries around the world, along with an additional 26 contracts to supply components for building 5G networks. Total income from sales that year was $108.5 billion.[3]

The second company in the field of building communications networks is ZTE, which was established in 1985 in Shenzhen. It was originally founded by the Ministry of Aerospace Industry as a straw company whose function was, inter alia, to send camouflaged agents overseas to collect technological information on aviation and space matters.[4] ZTE, like its larger competitor Huawei, already caught United States attention after it breached American sanctions and traded with North Korea and Iran through illegal deliveries of products and American technology. In early 2018, following long negotiations with the United States, ZTE was forced to absorb a severe economic blow when the US Department of Commerce banned American companies from selling components to it for the next seven years, and forced it to pay financial penalties, fire a number of senior executives, and agree to a mechanism for American supervision of its activity within the United States. The sanctions were a heavy blow for ZTE, which relies on essential parts made by American companies.[5]

Since the United States has no local manufacture of 5G communications infrastructure, it is therefore dependent on European companies to build its 5G networks.[6] In this situation, China can gain a significant edge in the future global communications market, including in the determination of standards and rules. The United States, which could find itself pushed out of its leading global position, is currently working energetically against the two Chinese communications company, in order to retain its technological advantage.

In this context, it is important for Israel to recognize and understand the latest trends in the rivalry between the powers, and in particular the position of the United States, which in recent months has pushed its allies "to choose a side" in the global race with intensive activity that is already bearing fruit, as other countries, mainly Western, accept the US position and boycott the Chinese communications companies for reasons of national security.

International Reactions

United States

The United States sees China as a competitor and rival, and there is a struggle between the two for global influence, economic competition, and technological leadership. Since 2007 members of the US Congress have adopted a hawkish attitude to the rise of Chinese communications companies, due to concerns about spying and the ability to shut down networks, and for economic reasons that could affect the profitability of American companies. In 2012 the House of Representatives Intelligence Committee called on Americans to avoid doing business with Huawei and ZTE, because of the allegedly significant cyber threat they represent to the United States.[7] Another complaint raised against ZTE was its refusal to give the Intelligence Committee documents concerning its business activity in Iran and North Korea. The committee called on regulators to block acquisitions on behalf of Huawei and ZTE, and recommended the removal of all Chinese-made software or components from security system computers due to espionage concerns. In 2018 the Trump administration also banned government employees from using cellular devices of Chinese manufacture.[8]

In July 2018, the *Globe and Mail* reported that the United States and Canada held talks to plan a consistent strategy in the attempt to prevent Chinese communications companies from controlling 5G infrastructure technologies.

These talks followed discussions held in the Five Eyes intelligence alliance, which includes Australia, Canada, New Zealand, Britain, and the United States. The newspaper reported that these countries agreed they should avoid relying on Huawei as sole provider for building communications infrastructure, because of its links with the Chinese government.[9] Moreover, the United States has recently started to put pressure on its allies to boycott the Chinese companies and stop them from building communications networks within their territory. For example, it was reported that members of the Senate Committee on Intelligence Matters had pressured the Prime Minister of Canada to thwart the involvement of Huawei in the construction of 5G networks. Senators Marco Rubio and Mark Warner, Republican and Democrat, respectively, wrote an official letter to the Prime Minister saying that "while Canada has strong telecommunications security safeguards in place, we have serious concerns that such safeguards are inadequate given what the United States and other allies know about Huawei."[10]

Australia and New Zealand

A notice issued by the Australian government in August 2018 did not mention the Chinese companies by name, but stated that "the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference."[11] Some two months later, Mike Burgess, the director-general of Australian Signals Directorate (ASD), which deals with foreign signals intelligence, argued that foreign communications companies should not be permitted to build 5G networks due to possible national security dangers. According to Burgess, Australia cannot allow the involvement of foreign companies in the construction of a sensitive communications infrastructure, since any breach due to infected components could shut down other sensitive infrastructures such as water, electricity, and health systems.[12] In addition to the concern over Chinese companies gaining access to communications, Australia is also working to deny these companies access to neighboring countries. For example, Australia forced the Solomon Islands to abandon a deal with Chinese communication companies in return for funding an undersea communications link.[13]

In November 2018, New Zealand also joined the countries boycotting Huawei when its intelligence agency notified its local communications

provider that it was banning it from using components made by Huawei to construct 5G networks, for reasons of national security.[14]

Britain and Elsewhere

In April 2018, the British National Cyber Security Centre (NCSC) issued a warning to the local communications industry not to use equipment and services from ZTE, as the equipment represents a threat to Britain's national security.[15] A report from the Huawei Cyber Security Evaluation Centre, a body set up by the British signals intelligence agency (Government Communications Headquarters) to assess levels of data security in Huawei's communications and broad band networks, claimed that "it is not possible to state with certainty that Huawei networks are not a danger to national security." The investigation found problems in the engineering processes of the Chinese company that "exposed new risks for British communications networks" and also "insufficient control of security of third party components."[16] Later, British Telecoms announced that it would remove Huawei components from its 3G and 4G networks over the next two years, and would not use Huawei components when setting up 5G networks in the future.[17] In response, Huawei undertook to invest $2 billion to allay the concerns of the British intelligence agency over use of its equipment and software. Senior officials in the Chinese company met with officials from the NCSC and agreed to a number of conditions that would lead to a change in the company's conduct in Britain.[18]

Other countries are also adopting the US position. In December 2018, Japan announced that it would boycott the Chinese communications companies and stop them from participating in building 5G networks there.[19] Similarly, the Indian Ministry of Communications announced that the Chinese companies would not participate in tenders to build Indian 5G networks.[20] However, other voices were also heard. Germany announced that it opposed any kind of boycott of communications providers,[21] and the French Minister of the Economy referred to Huawei when he said that they were welcome in France.[22] As of early December 2018, Canada was the only member of the Five Eyes Alliance that had not yet taken any steps to boycott the Chinese companies on its territory. Yet the arrest of senior Huawei executive Meng Wanzhou by the Canadian authorities has already led to a diplomatic crisis between China and Canada, and in retaliation China arrested three Canadian citizens.[23]

Chinese Involvement in Communications in Israel

The State of Israel, through the National Data Security Authority in the Israel Security Agency, does not allow China to build communications networks of any kind within the country, and Israeli communications companies have adopted the same security position and avoided introducing any Chinese parts into their equipment. This seems to indicate an unofficial Israeli policy against Chinese communications networks, for security reasons. However, there is no official policy regarding the installation of Chinese communications components within strategic infrastructure facilities such as ports and railway lines, which are built or operated by Chinese companies. Thus, in the context of the tender for the operation of the Haifa Port by the Chinese corporation SIPG, the Israel Ports company announced that the international operators were required to plan, fund, and set up the operating area of the port, including communications systems.[24] Similarly, in February 2018, NTA Ltd. (the Metropolitan Mass Transit System), which is responsible for construction of the light railway system in metropolitan Tel Aviv, announced that the Chinese CRTG Group had won the tender for the electricity and communications systems and the installation of light railway tracks.[25] Therefore, although there is some kind of ban on bringing Chinese communications infrastructures into Israel, it is not clear exactly how and to what extent it is enforced.

Moreover, Toga Networks of Hod Hasharon is actually operating as the Israeli development center of Huawei. The company develops switches and routers for telecom companies, cloud storage systems, and various applications for cloud based storage centers.[26] The presence of this kind of development center in Israel raises concerns that military information could reach the Chinese government, due to the possibility of the employment of graduates of IDF technology units who can contribute to the company from their military experience.

> The United States and its close partners see China in general and its communications companies in particular as a genuine threat to their national security. As such, the activity of these companies in Israel is bound up with direct dangers to national security and implications for relations with the United States.

Aside from the direct security issue, Chinese communications companies have a commercial foothold in Israel (table 1). For example, cellular devices from Chinese companies account for almost a fifth of the cellular market in Israel – a fact that illustrates the influence of Chinese companies on the Israeli economy.

Moreover, unlike the United States, military and government elements are not subject to a sweeping ban on the use of Chinese-made cellular devices. For example, in 2016 Meizu Ltd. was among the winners of the cellular tender to supply mobile devices to government ministry employees.[27] In addition, three Chinese companies, Xiaomi, ZTE, and Huawei, together invested tens of millions of dollars in Israeli technology companies engaged in Medtech, data security, and software.[28]

Table 1. Market share of Chinese communications companies in Israel, Q4 of 2018[29]

Chinese company	Importer in Israel	Market share
Huawei	Electra	3.74%
Xiaomi	Hemilton	12.26%
One Plus	Cell Now	1.31%
Oppo	No official importer	0.28%
Meizu	Bug	0.65%
ZTE	Eurocom	0.09%
Total share of Israeli cellular market		18.33%

When looking to the future, all the technologies and devices linked to the 5G network must be considered, and already a wide range of electronic devices made in China are sold in Israel. In Augut 2018, the importer Hemilton launched its first store for products from Xiaomi in Tel Aviv, offering various low priced devices such as electric scooters, televisions, and cameras.[30] This store is a further step in the entry of Chinese technologies into Israel, which could lead to Chinese control of information through various smart technologies, such as an electric scooter connected to a network that knows the user's location at any given moment, as well as civilian drones that are accessible to everyone and able to take photographs in sensitive areas.

Another issue that could represent a future danger is the involvement of cities and local councils in technological cooperation with China. For example, it was recently reported that a Chinese delegation that heard that Netanya was "among the most advanced places in the field of smart city management," wished to visit the city and examine options for strengthening business ties with it.[31] Smart city management is not unknown in China, which itself is a world leader in facial recognition technologies that are assimilated in its smart cities and help the local authorities to manage and control the population.[32] Chinese technology installed in tracking

cameras deployed in public areas have already led to suspicions that the data they collect could find its way to the Chinese government agencies. The assimilation of such systems in Israel could enable China to use its smart devices to sabotage operations and gain access to data through the various devices as one of the known weaknesses of the IoT, if and when it decides to exert influence on countries, companies, and individuals.

But in spite of the risks that Chinese technology poses for Israel, it is actually cooperation in the other direction – the sale of advanced Israeli technologies to China – that could be a greater danger, because of the risk that the United States could interpret it as aid to their big rival precisely in a field that is the core of the struggle between the two. While the transfer of Israeli military and dual use technologies to China is blocked entirely, the supervision of advanced civilian technologies is less strict, and their transfer to China could lead to a crisis in Israel's relations with both the United States and China.

Recommendations for Israel

In an era when Chinese communications companies led by Huawei are at the heart of an international storm, and when relations between the United States and China are at a low because of the trade war and the struggle over the future global technology market, the United States is ostensibly asking its allies all over the world to choose whether to support the US or China. At the moment it appears that US pressure is focused on communications, and it is indeed managing to influence its allies to boycott Chinese communications companies and prevent them from building 5G networks in those countries. The Chinese companies are absorbing severe blows in terms of their finances and image, but it is too early to assess how China will react to the current – and from its vantage, negative – trend. In the long run, China will likely continue to seek stability on the technological front, and will also use the current hostility to learn lessons and sharpen strategies. Even now it looks as if Chinese companies are prepared to make changes and adaptations in line with the rules in other countries.

The current involvement of Chinese communications companies in Israel is low, but it could increase thanks to the products they offer that are of good quality and attractive prices. Israel must remember that the United States and its close partners see China in general and its communications companies in particular as a genuine threat to their national security, and therefore the activity of these companies in Israel is bound up with

direct dangers to national security and implications for relations with the United States. In addition, Israel must give special attention to Chinese investments in other branches of advanced technology where Israel is at the forefront of development, and which the United States has marked as critical for its national security

At the same time, strong economic relations with China are highly important to Israel. In order to maintain good relations with both superpowers and avoid being injured in the struggle between them, Israel should pursue three objectives. First, it is particularly important to ensure an ongoing, serious dialogue with colleagues in the United States and Western countries, primarily through the security establishment and the intelligence community, in order to promote a joint view of the problem and ways to respond, and to incorporate their positions into policy. Second, the Israeli government must carry out a risk assessment and define suitable control mechanisms at all echelons of government in order to ensure proper adoption of advanced technologies, while also ensuring that advanced technologies such as artificial intelligence and cyber technologies do not find their way to unauthorized foreign entities. It was recently reported that the government is engaged in preparing a comprehensive regulatory protocol that will enable future foreign investments to be examined in a smarter way. This is a positive step, but it is important to guarantee that regulatory considerations are in line with United States demands on this subject. Third and no less important, Israel must assess the situation regarding its relations with China, in order to minimize any damage to Israel-China relations as a result of changes in Israeli policy. In this context too, there should be a mechanism for ongoing dialogue with the Chinese, to explain Israel's position and to prevent any unnecessary misunderstandings and loss of face for China.

Notes

1 David Shepardson, "Trump Signs Order to Set U.S. Spectrum Strategy as 5G Race Looms," *Reuters*, October 25, 2018, https://reut.rs/2OLXtfb.

2 Zoey Chong, "As 5G Looms, China's Already Looking at 6G Development," *CNET*, November 14, 2018, https://cnet.co/2B8q3Pm.

3 Jamie Davis, "Huawei Enters 2019 Swinging with $108.5 Billion Revenues," *Telecoms*, January 2, 2019, https://bit.ly/2TV3oNd.

4 Nick McKenzie and Angus Grigg, "China's ZTE Was Built to Spy and Bribe, Court Documents Allege," *Sydney Morning Herald*, May 31, 2018, https://bit.ly/2sqioX4.

5 Andrew Mayeda and Ian King, "U.S. Cuts Off China's ZTE From American Tech for Seven Years," *Bloomberg*, April 16, 2018, https://bloom.bg/2qEbgWe.
6 "The U.S., China and Others Race to Develop 5G Mobile Networks," *Stratfor*, April 3, 2018, https://bit.ly/2LTrB1P.
7 Charles Arthur, "China's Huawei and ZTE Pose National Security Threat, Says US Committee," *The Guardian*, October 8, 2012, https://bit.ly/2r7KlTK.
8 Jacob Kastrenakes, "Trump Signs Bill Banning Government Use of Huawei and ZTE Tech," *The Verge*, August 13, 2018, https://bit.ly/2vJAkyd.
9 Robert Fife and Steven Chase, "Ottawa Sees Chinese-owned Huawei as a Major Security Threat, Senior Official Says," *The Globe and Mail*, July 30, 2018, https://tgam.ca/2Orp8OB.
10 "U.S. Lawmakers Urge Canada to Snub China's Huawei in Telecoms," *Reuters*, October 12, 2018, https://reut.rs/2Cmlv7u.
11 Li Tao, "Australia Blocks China's Huawei, ZTE From 5G Development on Security Grounds," *South China Morning Post*, August 23, 2018, https://bit.ly/2o7scn8.
12 Gareth Hutchens, "Huawei Poses Security Threat to Australia's Infrastructure, Spy Chief Says," *The Guardian*, October 30, 2018, https://bit.ly/2CMMkmW.
13 Resty Woro Yuniar, "Australia's 5G Ban On China's Huawei, ZTE: Will Others Make Same Call?" *South China Morning Post*, September 7, 2018, https://bit.ly/2M7VcGA.
14 Vicky Xiuzhong Xu, "New Zealand Blocks Huawei, in Blow to Chinese Telecom Giant," *New York Times*, November 28, 2018, https://nyti.ms/2AtkM3n.
15 Andy Boxall, "U.K. Cybersecurity Agency Warns Against Using ZTE Telecom Equipment," *Digital Trends*, April 16, 2018, https://www.digitaltrends.com/mobile/zte-uk-security-threat-news/.
16 Annual Report, Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, HCSEC, July 17, 2018, https://bit.ly/2sp7GjY.
17 "BT Removing Huawei Equipment From Parts of 4G Network," *The Guardian*, December 6, 2018, https://bit.ly/2BVrO2L.
18 "Huawei Will Invest 2 Billion Dollars to Meet Britain's Security Demands," *Calcalist*, December 8, 2018, https://www.calcalist.co.il/internet/articles/0,7340,L-3751562,00.html.
19 Li Tao, "Japan Latest Country to Exclude Huawei, ZTE From 5G Roll-out Over Security Concerns," *South China Morning Post*, December 10, 2018, https://bit.ly/2MbbkXN.
20 Muntazir Abbas, "India Dials Cisco, Samsung, Nokia, Ericsson, Says No to Chinese Huawei, ZTE," *ET Telecom*, September 17, 2018, https://bit.ly/2paG7sW.
21 Ibid.
22 "Huawei Welcome in France, Sensitive Investments Can be Blocked: French Minister," *Reuters*, December 7, 2018, https://reut.rs/2SKLs79.

23 "China Warns Canada of 'Severe Consequences' Unless it Releases the Daughter of Huawei Founder," *Calcalist*, December 9, 2018, https://www.calcalist.co.il/world/articles/0,7340,L-3751596,00.html.

24 Lior Gutman, "The Chinese SIPG Wins Tender to Operate the New Port in Haifa," *Calcalist*, March 23, 2015, https://www.calcalist.co.il/local/articles/0,7340,L-3655245,00.html.

25 Lior Gutman, "Chinese and German Companies Win Tender for the Giant Systems of the Light Railway in Tel Aviv," *Calcalist*, February 19, 2018, https://www.calcalist.co.il/local/articles/0,7340,L-3732250,00.html.

26 Assaf Gilad, "Toga of Hod Hasharon Admits it is Chinese: A Branch of Huawei," *Calcalist*, March 22, 2016, https://www.calcalist.co.il/internet/articles/0,7340,L-3684098,00.html.

27 Sagi Cohen, "Why is Everyone Afraid of Huawei?" *The Marker*, December 10, 2018, https://www.themarker.com/technation/.premium-1.6727101.

28 Doron Ella, "Regulation of Foreign Investments and Acquisitions in Israel and Worldwide from a Comparative Viewpoint: China as a Test Case," in *Israel-China Relations: Opportunities and Challenges*, eds. Assaf Orion and Galia Lavi, Memorandum 185 (Tel Aviv: Institute for National Security Studes, 2018), pp. 62-65, https://bit.ly/2McMyqc.

29 Statcounter, December 2018, https://bit.ly/2Csoewc.

30 Ehud Keinan, "Xiaomi Store Opens in Tel Aviv: What Are the Prices?" *Mako*, August 14, 2018, https://www.mako.co.il/nexter-consumerism/Article-49b19b13da63561006.htm.

31 Barak Golan, "Showing Interest in Netanya: A Billion Chinese Can't be Wrong," *The Week in Netanya*, November 30, 2018, https://bit.ly/2DeWRal.

32 Scott N. Romaniuk and Tobias Burgers, "How China's AI Technology Exports Are Seeding Surveillance Societies Globally," *The Diplomat*, October 18, 2018, https://bit.ly/2TYOLIJ.