Photo: PIXABAY

Smart Cities with Chinese Characteristics

Hiddai Segev

The rapid growth of the global urban population demands more sophisticated management of both life in an urban setting and the resources in this environment—leading to the idea of "the smart city" that is equipped with a range of smart, advanced technologies. In recent years, Israel has also begun to develop plans for smart cities, which will lead inter alia to networked public spaces based on artificial intelligence systems. These systems are naturally potential information and cyber security risks, and risks to national security. Chinese companies export various smart city systems to dozens of countries, including Israel, notwithstanding Western allegations of breaches of human rights and dangers to national security. Israel should prepare a comprehensive national plan to map the existing situation, identify challenges and opportunities for the short and long terms, and manage risks relating to protection of privacy, data security, and cyber protection, from the strategic level down to the definition, deployment, and operation of individual systems.

Keywords: China, smart city, urban planning, artificial intelligence

According to UN estimates, by 2050 about 68 percent of the world's population will live in urban areas, almost 90 percent of them in Asia and Africa. This rapid growth of the urban population demands more sophisticated management of urban activity—i.e., more intelligent, ecological, and advanced. The idea of the "smart city" refers to efficient management of city life using advanced data analysis capabilities combined with artificial intelligence (AI), the internet of things (IoT), big data, and advanced communications networks. Smart cities strive to improve the quality, performance, and synchronization of municipal services, reduce costs and consumption of resources, and improve the interaction between citizens and authorities. For example, smart city technologies facilitate smart regulation of traffic and integrated management of emergencies.

Together with the progress and greater efficiency they offer, smart city technologies might also challenge individual privacy and increase the need for data security.

The concept of the smart city is based on a variety of technologies, built on what used to be called "the digital city," and on a range of applications constructed over the years. In 1974, Los Angeles developed the first urban big data enterprise, considered the first step in the history of smart cities. Twenty years later, in 1994, Amsterdam founded its own digital city venture, De Digitale Stad, and became the first digital city. In 2005 and with $25 million allocated over five years, Cisco became the first company to invest heavily in R&D on smart cities, and in 2008 the term "smart city" was introduced by IBM. In 2010 Japan chose Yokohama as a Next-Generation Energy Infrastructure and Social System Demonstration Area, and in 2011 the first Smart City Expo World Congress (SCEWC) opened in Barcelona. The global market in the field of smart cities is considered a growth market, and is expected to be worth over half a trillion dollars by 2027. The number of companies worldwide engaged in smart city apps is unknown, but an index of the top ten companies in the field includes technology giants such as Microsoft, Ericsson, IBM, Siemens, and Cisco.

Together with the progress and greater efficiency they offer, smart city technologies might also challenge individual privacy and increase the need for data security. For example, smart cameras deployed throughout the city can collect information and track residents, their way of life, and patterns of behavior using facial recognition and AI technologies. Infrastructures based more on sensors and remote control will become more widespread, with greater abilities to harbor personal data, thus increasing the risks of external cyber attacks seizing control or causing damage. Autocratic regimes can effectively exploit these technologies to reinforce their power and tighten control over their populations. Therefore, greater thought is necessary to define smart city policy in democratic countries, while creating facts on the ground, in order to avoid too much concentration of power in the hands of the authorities, to the detriment of the law, government, and the public.

Smart Cities in China

China is one of today's most advanced countries in the field of smart cities, and as of 2017, about half of the world's one thousand smart cities were in China. Data-based urbanization policy in China arose gradually according to technological developments and trends, both locally and worldwide, and above all, according to the evolving view of the Chinese Communist Party on the role of technology to maintain control and internal stability. China first presented the idea of the "digital city" in the 1990s, although the name was later changed to "the information-based city" and in 2009 was dubbed the "smart city" in the framework of the 12th five-year plan for China's economic and social development (2011-2015). In 2015 the idea of the "new smart city" appeared in China, as part of the 13th five year plan (2016-2020), which focuses on the integration of the IoT, big data, and cloud computing technologies.

Chinese President Xi Jinping has expressed his support for smart city initiatives, and in May 2017 stressed that China must "promote the development of cities and turn them into smart cities adapted to the 21st century." Xi also highlighted the Xiongan New Area—an urban venture launched in April 2017 south of Beijing, as the model for the future smart city and a symbol of new urban development in China. Today many of the leading companies in the fields of smart cities and AI operate in China, including Huawei, Megvii, Tencent, Hikvision, SenseTime, CEIEC, Alibaba, ZTE, Dahua, and Meiya Pico. The increasing number of Chinese companies engaged in the field of smart cities shows the importance of the field in the eyes of Chinese industry and government, which seek to set local and global standards, as with the 5th generation (5G) of cellular networks.

China is an autocratic country under the absolute control of the Communist Party, which has a grip on all governing authorities and every area of life, from policy to technological development. This necessarily affects the nature of smart cities in the country. A July 2020 study found that 18 of the most surveilled cities in the world are in China, with some 20 million tracking cameras as of 2017, and millions more to be installed in the near future. As AI, facial recognition, and big data technologies matured in recent years, China invested significant resources to build a "social credit" system, designed to incentivize desired behavior using carrots and sticks. This system is a kind of mass surveillance, and like the smart city systems, uses the same smart infrastructures deployed in the public space to monitor the population. The social credit rating is one aspect of the Communist Party's efforts to use advanced technology in order to monitor the public and reinforce its control, for the benefit of what it perceives as protection of national security and the public. The exact list of "unacceptable behaviors" has not been published, although there are reports of punishments for transgressors. These punishments include being denied the right to purchase airplane tickets, train tickets, public transport tickets, or even property. Moreover, the names of some of the companies mentioned above have been linked to assistance to the Chinese regime in its efforts to subjugate minorities in Xinjiang Province and northwest China.

Export of Chinese Smart City Systems

While deploying numerous smart city systems in its own territory, China also began to export them worldwide, as part of its 2015 Digital Silk Road strategic initiative (part of the Belt and Road Initiative). This digital initiative was designed to reinforce Chinese technological giants all over the world, build a Chinese-made digital infrastructure, and increase China's share of control of the global data and communications supply chain. In a 2017 speech, the Chinese President said that China's involvement in the development of smart cities in other countries was an opportunity to expand their economic cooperation with China. An October 2020 study found that since 2013 Chinese companies have exported smart city systems to 116 countries, including 38 Asian countries, 30 European countries, 15 Middle East countries, and 15 African countries. For example, in Bishkek, the capital of Kyrgyzstan, a special police command center has been established, equipped with smart systems supplied—at no cost—by the Chinese government's electronics corporation CEIEC; in Uganda, a contract worth $126 million has been signed with Huawei for the supply of smart city systems; in Uzbekistan a contract worth about a billion dollars has been signed with Huawei for the installation of 883 cameras, in addition to contracts with Huawei and ZTE for the assimilation of facial recognition technology in the country's education system. In Malaysia, Alibaba Cloud has installed an ET City Brain big data system, making Kuala Lumpur the first city outside China to deploy this system. Huawei has exported smart city systems to Italy, Germany, Holland, Spain, and France, while Hikvision has exported similar systems to the US, Britain, Demark, and Japan. In 2016, UTS University in Sydney signed a memorandum of understanding on smart city development with the CETC security corporation. As part of the Belt and Road Initiative, in October 2018 China signed an international "social credit alliance" with 35 cities in China, Italy, Mongolia, Myanmar, Saudi Arabia, France, and Thailand, with the aim of setting up a platform to coordinate the construction of a social credit system. Exporting the concept of social credit goes beyond the export of technology and products to the export of political and ethical concepts, and its management at the municipal level (links between municipalities) sometimes occurs under more lax supervision of aspects of foreign and security policy.

There has been much criticism of the Chinese systems worldwide, with claims that they export and spread the regime's norms, values, and methods.

The coronavirus crisis has given China the opportunity to export systems based on artificial intelligence. For example, Huawei supplied the Saudi government with a range of systems based on 5G and AI, and installed heat-tracking cameras in its hospitals and universities. In the UAE, the corporation supplied the municipality of Sharjah with autonomous vehicles to enforce and prevent public assembly. In Chile, Hikvision helped to install some 700 heat-tracking cameras all over the country.

Allegations against Chinese Smart City Systems

There has been much criticism of the Chinese systems worldwide, with claims that they export and spread the regime's norms, values, and methods. For example, in Serbia it was alleged that while Huawei's surveillance cameras with advanced facial recognition technology would significantly reduce crime, they could also be used by the regime to track journalists, political opponents, and human rights activists. A *Wall Street Journal* article of August 2019 found that Huawei employees themselves helped the authorities in African countries track opponents. In October 2019 the US Department of Commerce added 28 Chinese entities and technology companies to its black list, including some of the companies mentioned above, that have been linked to Chinese oppression and breaches of human rights against minorities in Xinjiang Province.

Western sources also claim that Chinese companies, both government and private, are required by Chinese law to assist the Communist Party and government ministries. For example, Article 7 of the National Intelligence Law (2017) requires "any organization or citizen [to] support, assist, and cooperate with state intelligence work in accordance with the law"; and Article 28 of China's Cybersecurity Law (2017) requires network operators to "provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law." Due to concerns that Chinese-made cameras are transmitting information to the Chinese authorities, some Western countries decided to limit their use. Cameras installed in sensitive military facilities in Australia and in US diplomatic missions all over the world have been removed over espionage concerns. Although Chinese companies deny that the government makes use of them for spying, in August 2018 the US administration decided on a sweeping boycott of Hikvision and Dahua products, for reasons of national security and public security. In November 2020 the US administration signed an Executive Order banning US investments in 31 Chinese companies, which are allegedly linked to or controlled by the Chinese security establishment, including Hikvision and Huawei.

In this framework, in August 2020 the US State Department announced the expansion of the Clean Network program that was launched the previous April, as part of the attempt to form a technology coalition of countries that agree with the need to secure their communications infrastructures, including future technologies, “by relying on only trusted vendors who are not subject to unjust or extra-judicial control by authoritarian governments, such as the Chinese Communist Party.” The initiative is intended to prevent the transfer of personal and business data of United States citizens to China to serve the interests of the Communist Party. The expanded initiative covers six areas that ban participation of Chinese companies: communications networks, communications providers, app stores, apps, cloud data storage, and underwater cables. Although the smart city is not explicitly mentioned in the US initiative, it is based on subsystems that interface with the fields mentioned, such as communications, cloud software, and data storage. The smart city, which by definition is part of the public space, affects the general public and involves numerous cyber and data storage risks, irrespective of who supplies the technology.

The broader context to the Clean Network is the deterioration in relations in recent years between the US and China, particularly during the Trump administration, in face of a strengtehing China. In a document of May 2020 entitled “United States Strategic Approach to the People’s Republic of China,” the US administration describes China as a challenge to the US economy, values, and security, and to the world order in general. Inter alia the document accuses China of forcing US companies and universities to transfer advanced technologies, and of waging cyber attacks to obtain such technologies. Furthermore, as its attitudes toward China become harsher, the US makes more demands on its allies to align with US policy and reinforce their risk management mechanisms with respect to China, buffered by warnings of an end to security and intelligence cooperation with the US should they not comply. As the US moves described above show, there is a trend toward technological decoupling. In this situation, the global system could be split into technological alliances that would limit their cooperation with companies and countries defined by them as national security risks. Indeed, the Clean Network plan ends with a call to US allies to join the initiative, which as of November 2020 included 53 countries, among them Israel, and 180 cellular providers with “clean” 5G communications networks.

Smart Cities in Israel

The government of Israel recognized the need to formulate a digital strategy back in 2013, as part of its economic-social strategy, and passed Resolution 1046. According to the 2020 annual report of the Ministry for Social Equality, in its early days the Digital Israel initiative operated from the Prime Minister’s Office, and then moved to the Ministry of Social Equality, and continues to operate from there. In 2016 the Ministry began studying the smart city concept with the Ministry of the Interior and local authorities. In 2018 a national digital plan was drawn up with a budget of over one billion shekels, including 144 projects such as smart cities, and designed to provide government support for the implementation of advanced technologies in local authorities. In December 2019 it was reported that a Smart City Innovation Center had opened in Tel Aviv. Moreover, Israeli-made smart city technologies are already in use in the country. For example, Taldor won a project for smart management of waste-removal systems for Eshkol Regional Council, while Axilion, in cooperation with a Microsoft subsidiary, has developed a smart city venture in Jerusalem. This venture, based on AI, manages the city’s traffic lights and streamlines the light railway traffic.

The State Comptroller’s report of May 2020 found that the government’s smart city national plan lacked a map of the existing situation, definition of the desired objective, and identification of challenges and opportunities.

The State Comptroller's report of May 2020 found that the government's smart city national plan lacked a map of the existing situation, definition of the desired objective, and identification of challenges and opportunities.

The report warned that there was no definition of an "inclusive element" to promote smart city ventures in Israel, and it was not clear how security considerations would be taken into account. Moreover, in Israel there was no official ban on the use of AI-based Chinese technologies, in addition to a lack of genuine government supervision of foreign relations at the municipal level. Thus there was nothing to stop Israeli local authorities basing their smart city systems on Chinese technologies, or even introducing them in partnership with Chinese cities. Indeed, cities such as Netanya, Ashdod, and Rishon Lezion previously announced cooperation or intended cooperation on technology with China, and they also maintain "twin city" links with Xiamen, Wuhan, and Tianjin, respectively. In 2017, a Chinese investment fund supported by the Kuang-Chi corporation, which inter alia engages in smart city technology, entered Israel. Chinese-made surveillance cameras are already in use in municipalities and in the Ministry of Labor, Social Affairs, and Social Services, and Chinese companies in this field are operating in Israel. For example, Hikvision has an agency called HVI Security Solutions that imports its products (its cameras were purchased by the Central Elections Committee in 2019), and the Huawei branch in Israel, Toga Networks, is also involved in the field of smart cities.

Conclusion and Recommendations

Among the many benefits afforded by smart city technologies are improvements to public life and more efficient control of local authority resources. At the same time, these technologies are accompanied by a variety of risks to national security and privacy, irrespective of the identity of the providers. In addition, the smart city raises concerns about possible harm to Israel's democratic values as the result of too much power in the hands of local authorities and political elements. It is therefore important to reinforce security, with an understanding that the smart city issue is too broad to be left entirely to the Ministry of Social Equality or the discretion of local authorities. The government must deliberate on the powers granted to elements that have access to the collected data, as well as the policy for using such data. There is a need for a comprehensive national plan and technology for smart technologies in the public domain, for a detailed picture of the smart city situation, for an analysis of the risks in terms of privacy, data protection, cyber defense, and national security, and a decision about applying the principles of the Clean Network to suppliers and systems in these areas.

Moreover, while local government in China, at the province and town level, is directly subordinate to the Chinese government, local authorities in Israel enjoy wide freedom of action in terms of foreign relations, with little government supervision. Therefore the Israeli government should review all foreign relations activity in local authorities with the emphasis on their assimilation of smart technologies, to ensure that national security and policy considerations are taken into account.

Finally, Israel must understand and monitor the implications of the developing policy of the Biden administration regarding the Clean Network, and thus seek to shift the debate on prohibitions to the discussion of strengthened partnerships in the age of superpower competition. Overall, it should aim to promote a strategic alliance on innovation and technology between the governments, higher education, and the private sector. Meanwhile trade with China, an important trading partner in many fields, should continue, without damage to Israel-China bilateral relations.

Hiddai Segev is a former researcher at INSS in the China program. hiddais@inss.org.il