Insight

One Eye on Zion, the Other on Beijing: Chinese Cameras in Israel

Yuval Less | No. 2143 | May 24, 2026

Camera networks in Israel are vulnerable to infiltration attempts by hostile actors, including Iran. The head of the National Cyber Directorate noted that since the beginning of the war, Iran and Hezbollah have been working jointly to hack security cameras across Israel for intelligence-gathering purposes. The information is used, among other things, to pinpoint missile strikes and target specific individuals. This highlights the dual-use nature of advanced cameras, particularly Chinese cameras originally designed for civilian needs yet carrying strategic potential for foreign intelligence and security agencies.

At the outset of the war with Iran on February 28, 2026, Israel carried out one of the most remarkable targeted killings in the history of modern warfare, eliminating Iran's Supreme Leader, Ali Khamenei. One of the key tools that aided Israeli intelligence was Tehran's traffic camera network, which was hacked and used for the systematic collection of information on the activities of the regime's senior leadership and the security circles surrounding them. Originally designed to monitor the public and suppress protests, this network became a significant intelligence asset that enabled the construction of an accurate situational picture. The information was analyzed using algorithms that identified senior officials' "patterns of life," while cameras provided critical angles for tracking their movements. On the day of the operation, these capabilities enabled precise, real-time identification of the target and his surroundings, contributing to the success of the elimination.

Israel's exploitation of Iran's camera network is not a new phenomenon, and officials in Tehran had previously warned that such systems could jeopardize national security, calling for stricter security controls on foreign-manufactured cameras. At the same time, this vulnerability is not unique to Iran, but rather reflects a broader phenomenon. Camera systems, particularly those connected to the network, are intended to enhance security and enable monitoring and control, yet they may also become points of vulnerability in the hands of a hostile actor for intelligence gathering and surveillance purposes. In the Israeli context, the widespread use of cameras, including foreign-manufactured technologies, highlights the potential exposure and the inherent security risk.

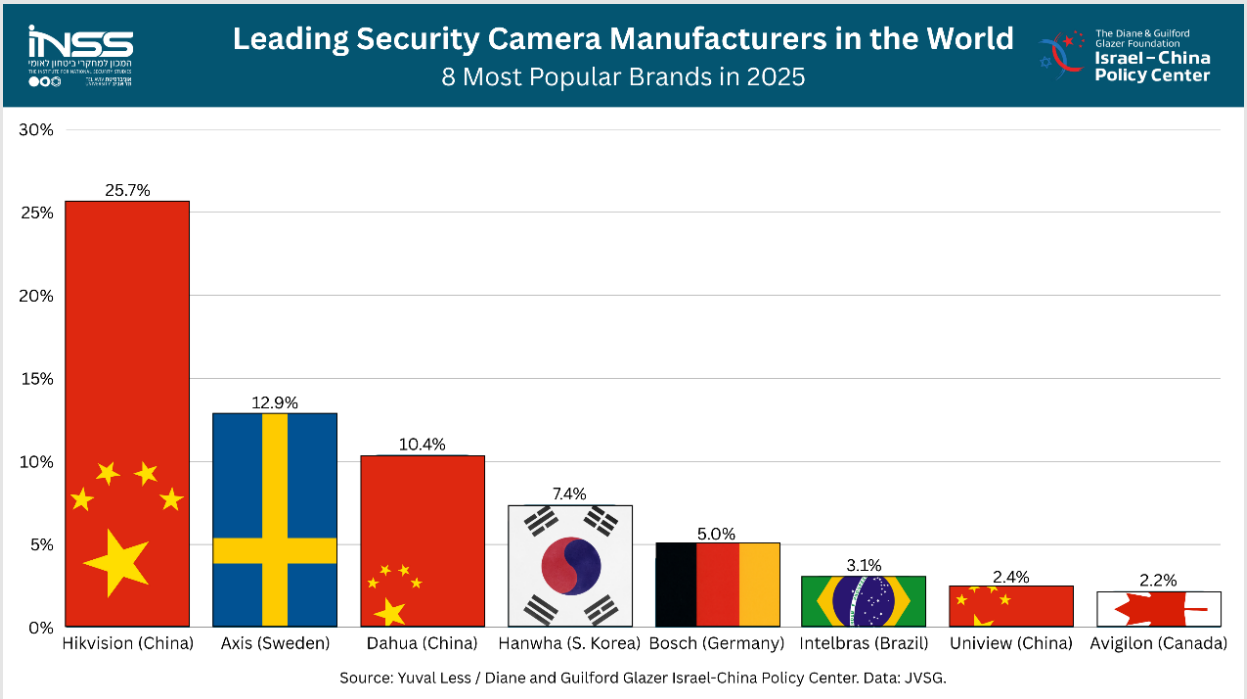
Chinese Cameras in Israel

Cameras are a central tool in the management and monitoring of public spaces, playing a significant role in security, transportation, and law enforcement. The new generation of cameras, based on Artificial Intelligence and IoT systems, no longer merely records events passively, but also analyzes and identifies activity in real time, enabling the detection of patterns and anomalies and supporting rapid decision-making. Alongside the advantages, these systems are exposed to security weaknesses, remote takeovers, data leaks, and privacy infringements. Connecting cameras to the cloud and allowing remote access increases the risk of information being exploited by hostile actors. Compared to other IoT devices—such as basic sensors (i.e., temperature, motion, and light sensors) and "smart home" devices (including smart lights and locks)—advanced cameras collect information on a much broader scale. As a result, they may serve as "eyes and ears" for a hostile actor, facilitating intelligence gathering, surveillance, and support in operational planning.

In Israel, the exposure risks stemming from camera usage are amplified given the security context and the country's status as a prominent target for cyberattacks by foreign entities. In recent years, security officials have warned against attempts to exploit cameras for intelligence gathering on sensitive locations and movements. While security risks exist across all types of cameras, regardless of the manufacturer or country of origin, the Chinese challenge adds another layer of complexity and presents unique technical and geopolitical issues that warrant a re-examination of the risks associated with the use of Chinese-made technologies.

China has become a superpower in the production and deployment of security cameras. The scale of operation and government investment, combined with competitive pricing and high performance, have enabled China to establish an advantage and foster leading companies, including Hikvision and Dahua, which together account for more than 30% of the global manufacturing market share (see Graph A).

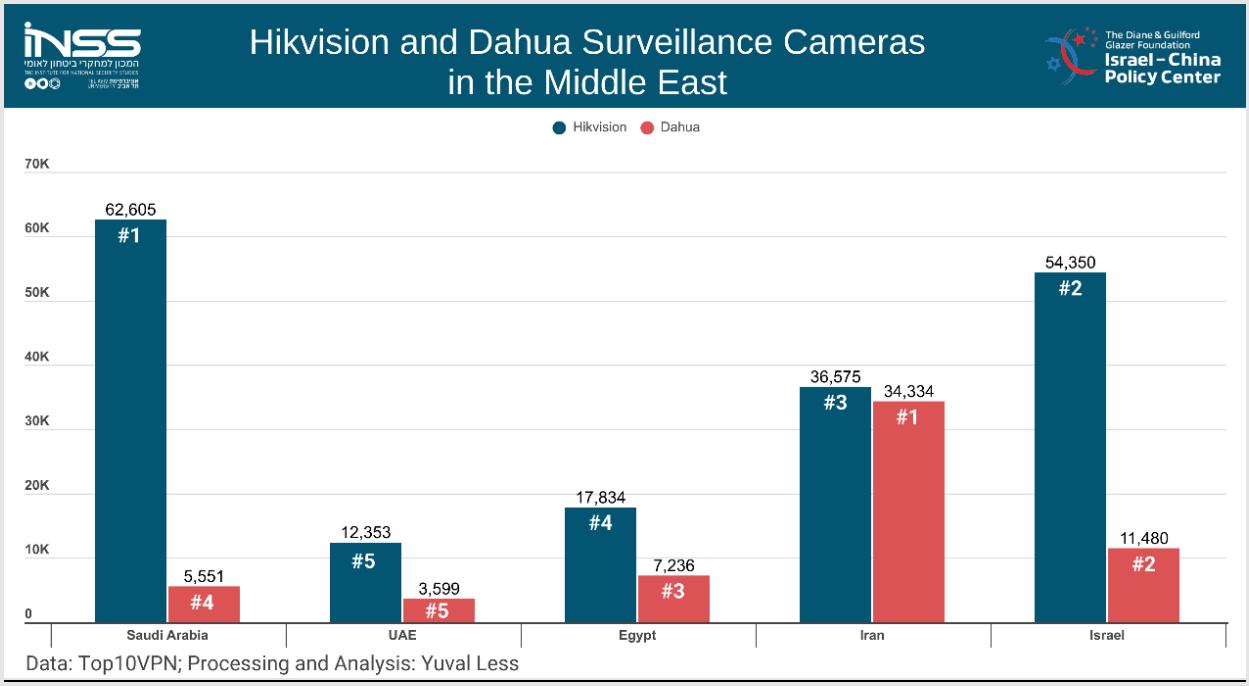
Graph A:



According to 2025 data from JVSG, a video surveillance and security system design platform based on actual usage data, the Chinese company Hikvision dominates approximately 25.7% of the global market. It is followed by Axis Communications from Sweden (12.9%), Dahua from China (10.4%), Hanwha from South Korea (7.4%), Bosch from Germany (5.0%), Intelbras from Brazil (3.1%), Uniview from China (2.4%), and Avigilon from Canada (2.2%). China's rise as a leading manufacturer in the field of surveillance cameras serves as a technological pillar within a broader strategy aimed at exporting technologies and promoting Chinese standards, as part of Beijing's wider effort to expand its global influence.

The presence of Chinese-made cameras is evident throughout Israel's public and private sectors, including public transportation systems, educational and healthcare institutions, residential buildings, and even sensitive sites such as government offices and border crossings. As part of the 'Hawk Eye' project, the Israel Police uses advanced license plate recognition cameras, including cameras manufactured by Dahua and systems produced by Hikvision. In 2021, Top10VPN, a British research organization specializing in digital tracking, privacy, and surveillance technologies, published a report mapping the deployment of security cameras manufactured by Hikvision and Dahua outside of China, including in the Middle East. According to the findings, approximately 65,830 cameras produced by these companies are installed in Israel, of which roughly 54,350 cameras are manufactured by Hikvision and approximately 11,480 are manufactured by Dahua (see Graph B).

Graph B:



For Israel, the use of Chinese cameras presents a range of political, technological, and geopolitical challenges, highlighting the implications of relying on foreign technology in a manner that demands increased attention from government and security authorities.

The first challenge relates to the political aspect and stems from the close ties between the Chinese government and technology companies. In China, both state-owned and private companies operate in close alignment with state mechanisms, meaning that business interests are intertwined with strategic

objectives. Hikvision, for example, is controlled by the Chinese state-owned conglomerate, China Electronics Technology Group Corporation (CETC), which also serves the defense industry, while senior company officials simultaneously hold positions within the Chinese Communist Party and government bodies. Dahua, although not fully state-owned, also maintains ties to the government and the defense establishment. Both companies operate within an environment in which alignment with the Party and the state is an inherent part of their structure, effectively blurring the line between commercial activity and national interests. This relationship is also anchored in a legal framework that obligates companies in China to cooperate with state authorities and hand over information upon request. Laws including the Counter-Espionage Law (2014) and the National Intelligence Law (2017) institutionalize this obligation and heighten concerns that information collected through Chinese technologies could be accessible to government authorities in China.

Second, the technological challenge posed by China manifests primarily in security vulnerabilities. Although vulnerabilities exist across all types of cameras, studies indicate that in Chinese-manufactured cameras, including those produced by Hikvision and Dahua, such vulnerabilities are sometimes more severe and complex to address. A study published in the Journal of Cybersecurity found flaws in authentication and authorization mechanisms, the use of default passwords, and vulnerabilities enabling unauthorized access, code execution, and data leakage. Part of the issue stems from complex update processes and the absence of advanced security mechanisms by default. Additionally, these cameras have fewer layers of protection while simultaneously running numerous open services, thereby increasing the attack surface by expanding the number of potential entry points into the system and making it easier for attackers to identify and exploit existing vulnerabilities.

These vulnerabilities raise security concerns given the deepening strategic ties between China and Iran, as well as the fear that Iranian actors could exploit such vulnerabilities against Israel. In recent years, the United States has warned against the use of Chinese technologies, with the U.S. Department of Homeland Security (DHS) cautioning that Chinese-manufactured cameras could serve as a means of espionage against critical infrastructure.

The third challenge, geopolitical in nature, stems from the growing technological competition between China and the United States. Hikvision and Dahua are included in the FCC's Covered List in the United States, which identifies communications and technology equipment manufacturers considered to pose risks to national security due to their ties to the Chinese government and defense industry. Their inclusion on this list leads to significant restrictions, including bans on the authorization and marketing of new equipment, limitations on their use in government systems, and the removal of existing equipment from sensitive facilities. At the same time, the United States has imposed sanctions on Chinese companies, including Hikvision, Dahua, Uniview, and Tiandy, over their involvement in civilian surveillance and repression projects within China.

Other countries around the world have joined the United States in efforts to remove Chinese equipment from sensitive sites and critical infrastructure. For example, the United Kingdom directed the removal of Hikvision and Dahua equipment from sensitive government buildings and prohibited their installation at defense sites; Australia led efforts to remove Chinese cameras from government offices and critical infrastructure; Canada restricted the use of Chinese equipment in federal institutions and re-examined existing contracts; and India barred Chinese vendors from participating in certain

government projects, while favoring alternative domestic vendors on national security grounds. In Israel, by contrast, no comprehensive policy has yet been formulated regarding the use of Chinese-made cameras. Against the backdrop of these global steps, Israel must prepare for the possibility of American pressure to reduce its reliance on Chinese technologies and evaluate the alignment of its policy with technological cooperation frameworks involving the United States and Western countries, including initiatives such as Pax Silica.

Conclusions and Recommendations

China holds critical positions within the global manufacturing and supply chain for security cameras, making complete technological decoupling impractical, particularly given that Chinese components are also integrated into many Western products. This complexity is further compounded by the phenomenon of white labeling, which blurs the true origin of the technology and complicates efforts to assess their security level. In addition, within an open market, the state's ability to oversee technologies used in the private sector is inherently limited. Consequently, a strategy of informed risk management should be adopted, one that promotes practical measures aimed at reducing exposure to the risks associated with reliance on Chinese technology.

- **Transition to Western Alternatives:** At security sites and critical infrastructure, Israel should promote a gradual transition to non-Chinese alternatives in order to reduce security risks at strategic locations. In addition, Israel's defense establishment should implement an orderly transition toward non-Chinese alternatives, even at an economic cost. In particular, projects such as the Israel Police's "Hawk Eye," which rely in part on Chinese-made systems, illustrate the scale of usage of these technologies and the need to reassess the extent of this reliance. These alternatives could be based on domestic or Western vendors.
- **Strengthening Domestic Industry:** Israel should encourage the development and production of domestic security infrastructure, cameras, software, and surveillance-related services. Such a move could help reduce dependence on imports and improve control over the supply chain, while also strengthening Israel's technological capabilities. In this context, efforts should focus on fostering an ecosystem built on Israeli and Western solutions, while integrating components sourced from trusted suppliers.

Editors of the series: Anat Kurz, Eldad Shavit and Keri Rosenbluh