CIVIC IDEA

Exporting Technological Authoritarianism:

How Chinese Technology Is Integrating into Georgia's State Infrastructure

2026

Table of contents

Exporting Technological Authoritarianism:
How Chinese Technology Is Integrating into Georgia's State Infrastructure

The deployment of surveillance systems creates a strategic foundation for state governance and data collection. The transparency and accountability of this process directly determine the quality of governance.

Accordingly, the integration of highly sensitive technologies into state infrastructure goes beyond an administrative framework and constitutes a fundamental political choice between democratic standards and authoritarian order.

In recent years, international discourse has intensified around the risks associated with digital and surveillance technologies produced by authoritarian states, particularly the People's Republic of China. Against this backdrop, the introduction of such systems into Georgia's state infrastructure is becoming a complex challenge, as it simultaneously concerns national security and data sovereignty.

Civic IDEA has been monitoring the process of integrating Chinese technologies in Georgia for years. The present research, covering the period from 2025 through March 2026, is based on a detailed analysis of public procurement records.

The purpose of the study is to examine the scale of the spread of Chinese-made video surveillance systems, identify the main manufacturing companies, and assess the risks generated by the expansion of the Chinese digital ecosystem.

The research identified several trends that define the scale and character of the spread of Chinese technologies in Georgia:

• Chinese-made surveillance equipment and digital devices are widely and systematically embedded in Georgia's public sector.

2025 –March 2026 ○——○ **23 public procurements**

• Intensive and systematic procurements of Chinese-made surveillance equipment are observed at the level of local self-government bodies, namely municipalities;

An examination of public procurement dynamics shows that the uptake of Chinese technology in the public sector is concentrated around several major hubs. In particular, the study identified several key institutions whose spending on Chinese technologies from 2025 through March 2026 significantly exceeded the figures recorded by other public organizations:

Category	Institution	Equipment Type	Total Spending (GEL)
Specialized Agency	Kutaisi Municipality City Hall	Surveillance systems	6,600,795
Specialized Agency	NNLE Department of Urban Infrastructure and Improvement	Surveillance systems	1,972,300
Education / Training Institution	National Assessment and Examinations Center	Surveillance equipment	340,933
State Agency (Environmental / UAV use)	Agency of Protected Areas	Unmanned aerial vehicles (UAVs)	231,068

Among the manufacturers integrated into Georgian state infrastructure are companies known internationally for their questionable reputations. These include:

- Hangzhou Hikvision Digital Technology Co., Ltd
- Zhejiang Uniview Technologies Co., Ltd
- Tiandy Technologies
- SZ DJI Technology Co., Ltd
- Autel Robotics

The integration of Chinese-made surveillance and other types of equipment with questionable reputations into state infrastructure is associated with several key risk factors:

- According to CISA and the FBI, the integration of Chinese technologies into critical infrastructure creates the risk of covert access to data;
- Chinese companies have a legal obligation to cooperate unconditionally with China's intelligence services;
- According to assessments by international organizations, the introduction of Chinese critical systems in fragile democracies creates the risk of political control and the adoption of repressive practices.

The above-mentioned factors create a complex context in which research into the integration of Chinese-made technologies in the state sector becomes essential.

Chinese-Made Surveillance and Digital Technologies in Public Procurement

In the process of modernizing technological infrastructure in Georgia's public sector, the introduction of Chinese-made surveillance systems and specialized digital devices has become one of the significant trends.

An analysis of public procurement data from 2025 through March 2026 shows that the technological equipping of public institutions is significantly linked to Chinese manufacturers and their products. The trend indicates that this equipment is firmly integrated across different institutional levels of the Georgian government.

Municipal Procurement: The Geography of Chinese Technology Expansion

Procurements carried out at the municipal level clearly illustrate the trend of using Chinese-made surveillance equipment. Existing practice shows that the introduction of these technologies is a systemic process that covers various regions of Georgia.

Municipal Procurement of Chinese-Made Technologies (2025–March 2026)

Date	Municipality	Amount (GEL)	Equipment Type	Manufacturer	Supplier
June 2025	Kutaisi	6,600,795	Surveillance system	Xiamen Milesight IoT Co., Ltd	Delta Consulting
Dec 2025	Kutaisi	795	School equipment	Shenzhen TVT Digital Technology Co., Ltd	Bedi.ge
July 2025	Khobi	69,968	Video-conference camera	Guangdong Baolun Electronics Co., Ltd	Mifasi
Sept 2025	Khulo	58,374	Surveillance system	Zhejiang Uniview Technologies Co., Ltd	UGT
Dec 2025	Khelvachauri	900	IP cameras	Shenzhen TVT Digital Technology Co., Ltd	Bedi.ge
March 2026	Ozurgeti	31,240	IP cameras & devices	Tiandy Technologies	G.L.M Group

Thus, the data show that the integration of Chinese surveillance systems into state infrastructure is not merely a static reality, but a growing trend over time, spanning multiple regions of Georgia.

Chinese Technological Expansion in the Public Sector

The overall dynamics of individual procurements carried out by state agencies confirm that the introduction of Chinese-made video surveillance systems is a widespread practice beyond municipal units, extending across almost every type of state structure.

Chinese surveillance systems are widely integrated into the education sector. In this area, one of the largest and regular purchasers of equipment is the National Assessment and Examinations Center. All Chinese-origin equipment purchased by the agency was manufactured by Hangzhou Hikvision Digital Technology, while the supplier company was LLC Neotech.

Procurement in Education and Training Institutions (2025–March 2026)

Date	Institution / Agency	Amount (GEL)	Equipment Type	Manufacturer	Supplier
July 2025	National Assessment and Examinations Center	17,012	Network cameras & recording devices	Hangzhou Hikvision Digital Technology Co., Ltd	LLC Neotech
July 2025	National Assessment and Examinations Center	19,296	Network cameras & recording devices	Hangzhou Hikvision Digital Technology Co., Ltd	LLC Neotech
Dec 2025	National Assessment and Examinations Center	304,625	Network cameras & recording devices	Hangzhou Hikvision Digital Technology Co., Ltd	LLC Neotech
July 2025	Tbilisi State University	5,547	Conference camera	Kandao Technology Co., Ltd	LLC CityTech
Oct 2025	Tbilisi State University (College of Media & TV Arts)	15,995	Compact video camera & auxiliary equipment	SZ DJI Technology Co. Ltd	G.L.M Group
Nov 2026	General Giorgi Kvinitadze Cadet Military Lyceum	19,370	Video recording & auxiliary equipment	Hangzhou Hikvision Digital Technology Co., Ltd	LLC ITCraft
March 2026	Sighnaghi Municipality Complex Sports School	10,777	17 video cameras & auxiliary devices	Hangzhou Hikvision Digital Technology Co., Ltd	LLC Nanotech Georgia

Beyond educational and academic institutions, the spread of the Chinese surveillance ecosystem is also taking place in specialized agencies whose activities are connected to field monitoring and infrastructure management.

Procurement in Specialized Agencies

Date	Institution / Agency	Amount (GEL)	Equipment Type	Manufacturer	Supplier
June 2025	N(N)LE Department of Urban Infrastructure & Improvement	1,972,300	370 surveillance video cameras	Xiamen Milesight IoT Co., Ltd	LLC Delta Consulting
July 2025	Animal Monitoring Agency	11,975	Shoulder-mounted body cameras	Shenzhen Eeyelog Technology Co., Ltd	LLC CityTech
Dec 2025	Department of Environmental Supervision	19,560	Vehicle surveillance systems	Streamax Technology Co., Ltd	LLC Lumeni
Feb 2026	Maritime Transport Agency	10,395	150 webcams	TRUST INTERNATIONAL B.V.[1]	LLC IT Tech

The procurement of video surveillance systems and auxiliary devices is not limited to public institutions. Similar practice is also visible in the activities of state-owned enterprises and municipal institutions.

Procurement in State-Owned Enterprises and Municipal Institutions

Date	Institution / Agency	Amount (GEL)	Equipment Type	Manufacturer	Supplier
May 2025	LLC Georgian Amelioration	7,995	Outdoor surveillance cameras	Shenzhen TVT Digital Technology Co., Ltd	Safe X
July 2025	LLC Batumi Water	10,769	Surveillance cameras & auxiliary devices	Zhejiang Uniview Technologies Co., Ltd	LLC IT-Craft

1. Note: TRUST INTERNATIONAL B.V. is a Dutch company; however, its products are manufactured in Chinese factories.

Thus, it is evident that Chinese-made surveillance technologies are systematically integrated into Georgia's public sector. This expansion covers critical infrastructure, military-educational institutions, and regional services alike, indicating a high level of technological dependence among state agencies on Chinese manufacturers.

Beyond Video Surveillance Systems: Unmanned Aerial Vehicles and Other Digital Devices

The use of Chinese technologies in the public sector is not limited to stationary video surveillance systems. Public procurement data show that state agencies actively use Chinese-made unmanned aerial vehicles and other digital devices, further expanding the area of technological dependence.

Procurement in Protected Areas and Education Sector

Date	Institution / Agency/ Entity	Amount (GEL)	Equipment Type	Manufacturer	Supplier
July 2025	Agency of Protected Areas	110,000	5 thermal drones	Autel Robotics Co. Ltd (AUTEL)	LLC TMLnet
Aug 2025	Agency of Protected Areas	100,300	4 thermal drones	Autel Robotics Co. Ltd (AUTEL)	LLC Bedi.ge
Sept 2025	Agency of Protected Areas	20,768	1 thermal drone	Autel Robotics Co. Ltd (AUTEL)	LLC My Mobile +
July 2025	N(N)LE Akaki Chkhaidze Art School	450	Barcode scanner	SUNLUX IOT Technology (Guangdong) Inc.	LLC RS Line

Accordingly, Chinese technological expansion in Georgia's public sector has a systemic character at both the municipal level and across various state agencies. The integration of surveillance systems, thermal drones, and specialized digital devices in critical areas such as security, education, and strategic infrastructure indicates the growing technological dependence of state agencies on Chinese manufacturers. According to 2025-2026 data, this dynamic remains unchanged.

The Chinese Surveillance Ecosystem: Profiles of Technology Manufacturers

The market for the supply of Chinese-made digital technologies in Georgia is distributed among several companies, although these entities mostly function only as local integrators. Accordingly, the analysis of the research cannot be complete without examining the profiles of the companies whose products are integrated into Georgia's state sector.

Several manufacturing companies appear among the Chinese devices purchased by Georgian state agencies whose **activities are associated internationally with high security risks.** In international practice, these companies have repeatedly become the subject of criticism.

The list of these companies is as follows:

Hangzhou Hikvision Digital Technology Co., Ltd is one of the world's largest manufacturers of video surveillance systems and was added to the U.S. Department of Commerce's Entity List as early as 2019. The company is accused of involvement in the Chinese government's repression and mass surveillance of Uyghur Muslims. In addition, since 2021, the U.S. Federal Communications Commission (FCC) has considered Hikvision products an "unacceptable risk" to national security under its Covered List.

In 2025, the Government of Canada ordered Hikvision Canada to cease operations on national security grounds, while in 2023 the Australian Department of Defence stated that Hikvision-made cameras would be removed from government sites.

Zhejiang Uniview Technologies Co., Ltd (UNV) is one of the major manufacturers in China's video surveillance and AIoT sector. The company's reputation is under question because Uniview technologies have appeared in a number of investigative and research materials. According to IPVM, Uniview technologies were actively used in systems for ethnic identification and surveillance.

Against this backdrop, in December 2024, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) added Uniview to the Entity List on the grounds that the company participated in "high-technology surveillance" targeting the general population as well as Uyghurs and other ethnic and religious groups.

Tiandy Technologies came under international scrutiny in 2022, when the U.S. Department of Commerce's Bureau of Industry and Security (BIS) added it to the Entity List. According to the Federal Register, the sanctions against the company were prompted by its involvement in repression in the Xinjiang region, as well as its role in facilitating the acquisition of U.S.-origin products and technologies for Iran's Islamic Revolutionary Guard Corps.

SZ DJI Technology Co., Ltd, the world's largest manufacturer of unmanned aerial vehicles, has been on the U.S. Department of Commerce Bureau of Industry and Security's Entity List since 2020. According to the Federal Register, DJI was included among entities that enabled high-technology surveillance and human rights violations.

From an international security perspective, substantial concerns exist regarding the company's transfer of data to Chinese intelligence services and the dual-use application of its technologies in the war in Ukraine. Taking these risks into account, DJI also appears on the U.S. Department of Defense (DOD) list of "Chinese military companies".

Autel Robotics has become the object of growing attention in Western political and regulatory circles in recent years. In 2024, an initiative emerged in the U.S. Congress to ban new drones manufactured by the company from entering the U.S. market, a move linked to data security risks.

In 2024, the company was added to the U.S. Bureau of Industry and Security's Entity List. According to the official explanation, this decision was driven by the company's involvement in supplying controlled components to Russia, as well as attempts to procure U.S. products for unmanned aerial vehicles (UAVs) connected to Chinese military entities.

In addition, Autel Robotics Co., Ltd appears on the U.S. Department of Defense's 2025 list of "Chinese military companies". In parallel, the FCC's 2025-2026 decisions further tightened regulations concerning foreign-made unmanned aircraft systems (UAS), which Autel is publicly contesting.

Sanctioned, Blacklisted , Entity List (U.S. Department of Commerce), Covered List (FCC), Restricted, National security concern, High-risk surveillance technology, Human rights concern designation.

Technological Sovereignty or Systemic Threat?

The integration of Chinese-made technologies into state infrastructure is a complex challenge in which security-related risks are determined by several interlinked factors.

According to the Atlantic Council, the spread of Chinese surveillance technologies is not merely the export of individual devices, but the expansion of a "surveillance ecosystem", in which state interests, the private sector, and technological infrastructure function as a single, synchronized system.

The use of these products in the state sector is associated with several main risk factors:

The Digital "Trojan Horse": Cybersecurity and the Risk of "Covert Access" to Data

In the digital era, software is not merely a functional tool; it is one of the fundamental pillars of modern device security. A technical threat is created by the existence of pre-integrated vulnerabilities in systems, which allow third parties to gain covert access to data. This calls into question informational integrity and systemic resilience. Specifically, an official joint guidance document by CISA and the FBI directly addresses Chinese-made drones and states that they pose a "significant risk" to critical infrastructure. The document notes that the operation of such systems may make sensitive information accessible to the Chinese government.

FBI Director Christopher Wray and CISA Director Jen Easterly view this threat in a broader strategic context. According to Christopher Wray, China seeks to cause panic by "striking civilian infrastructure" in a crisis situation. Jen Easterly stated that Chinese cyber actors, including Volt Typhoon, are penetrating "deep into" U.S. critical infrastructure in order to carry out destructive actions during a crisis or conflict.

The realism of this threat is also confirmed by recent experience. According to a 2024 joint statement by the FBI and CISA, the networks of several American telecommunications companies became targets of a cyberattack by China-affiliated actors. According to the agencies, the attackers obtained data related to customer call records, penetrated the private communications of certain individuals in government and political circles, and also gained access to certain information related to law enforcement court requests.

The case demonstrates that penetration into critical data flows through civilian and commercial infrastructure is not merely a hypothetical threat; it has become a real challenge for state security and the protection of informational sovereignty.

Chinese Legislation: A Legal Obligation to State Control

One of the most frequently cited and critical issues in assessing Chinese technologies is the country's legal environment:

- Under the 2017 National Intelligence Law, all organizations and citizens are required to "support, assist, and cooperate with" national intelligence activities, while the law grants state security bodies the authority to demand such cooperation;

- The 2021 Data Security Law significantly strengthens state oversight over data processing and expands the authorities' access to and control over digital assets owned by the private sector;

The legal environment is especially sensitive for state agencies, because existing research confirms that China's legislative framework is not merely a local regulation, but a global-scale technological risk factor. The Australian Strategic Policy Institute (ASPI) emphasizes that China's legal system does not provide for independent judicial oversight, leaving companies without a legal lever to refuse requests from state security bodies. In parallel, the Center for Strategic and International Studies (CSIS) notes that China's national security system legally obliges civilian and military sectors to cooperate with each other, thereby turning Chinese technology companies into an organic part of the state intelligence system.

Additionally, a legal analysis prepared by Mannheimer Swartling notes that the National Intelligence Law has an extraterritorial character and may potentially extend to the foreign subsidiaries of Chinese companies and to data processed abroad by them. At the same time, an Atlantic Council report states that China's 2021 Data Security Law further strengthens central government control mechanisms over the private sector's digital assets and data.

Accordingly, the overall conclusion of the cited studies is clear: for Chinese manufacturers, "collaboration" with state interests is not a choice, but a legal obligation, which in practice nullifies guarantees of data integrity for international partners.

Human Rights and Democratic Standards: The Ethical Dimension of Technological Export

Decision-making on technological solutions in the state sector goes beyond economic or functional considerations and is directly connected to democratic values and human rights protection. The risk increases when technology is integrated into environments where data protection guarantees are weak and independent oversight is limited.

According to the Carnegie Endowment for International Peace (CEIP) study, The Global Expansion of AI Surveillance, Chinese companies, including Huawei, Hikvision, Dahua, and ZTE, are among the main suppliers of AI surveillance technologies worldwide. The study emphasizes that such surveillance tools often become mechanisms of political control in countries characterized by fragile democratic institutions.

Freedom House views this process in a broader political context and describes it as the export of "digital authoritarianism". According to the organization, the Chinese model involves the spread of internet governance practices based on large-scale censorship, surveillance, and the mass collection of personal data.

Accordingly, the integration into state infrastructure of Chinese technologies associated with systemic human rights violations is not merely a technical or administrative decision. It also constitutes an ethical and political choice that determines institutional credibility, the state's value orientation, and its commitment to principles of democratic governance.