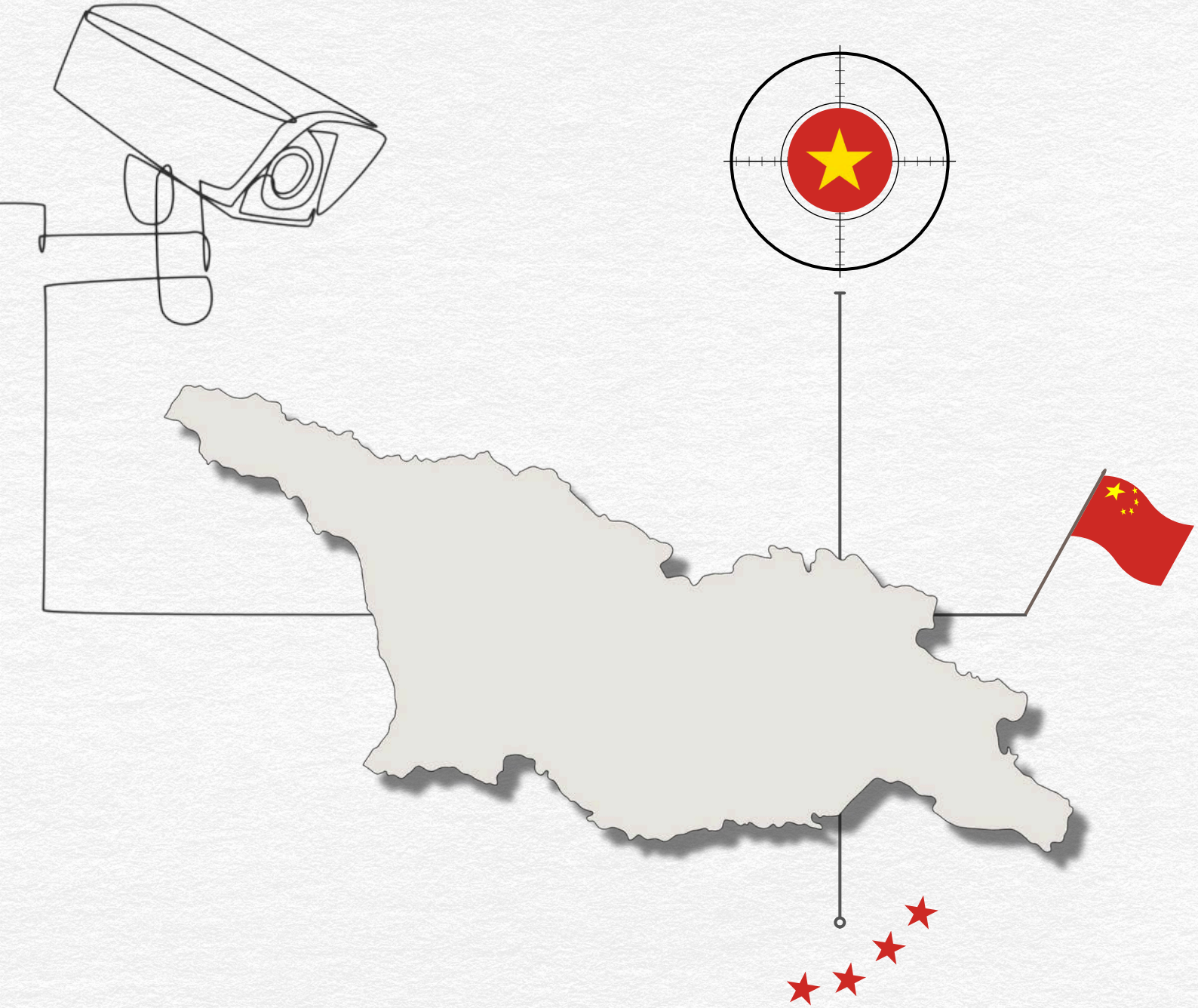
EMERGING CONCERN

Chinese Surveillance Cameras in Georgia



Tbilisi

January 2025

Author:
Aksana Akhmedova

The illegitimate Georgian Dream (GD) government's increasingly anti-Western foreign policy is becoming more evident in the evolving dynamics of Sino-Georgian relations. While improving Georgia's **alignment** with the EU's Common Foreign and Security Policy is crucial for Euro-Atlantic integration, the GD's current foreign policy priorities contradict this objective. Cooperation with an authoritarian regime, specifically the People's Republic of China (PRC), in areas such as law enforcement, defense, and security jeopardizes not only Georgia's national security but also its EU integration process.

Civic IDEA will continue its research and share further findings with you in 2025. For now, we focus on a specific aspect of law enforcement cooperation: **the growing prevalence of surveillance cameras produced by Chinese companies in the Georgian market.** These technologies pose significant cybersecurity threats and potential data breaches, raising serious implications for national security. The close alignment of prominent technology companies with the Communist Party of China further intensifies these concerns. The following facts reinforce these issues:

- Chinese surveillance camera manufacturers, such as Hikvision and Dahua, are subject to Chinese laws, including the 2017 National Intelligence Law, which mandates companies to cooperate with the Chinese government when requested. This raises concerns that data collected by these cameras could be shared with Chinese intelligence agencies.

- There are concerns that PRC-manufactured surveillance systems could be exploited for espionage. Backdoors or vulnerabilities intentionally built into these systems could enable the Chinese government to monitor or infiltrate critical infrastructure or sensitive facilities. These systems could create significant vulnerabilities to foreign interference or sabotage if integrated into key areas, such as government buildings, military bases, or transportation hubs.

- Democratic states in the West argue that Chinese surveillance technologies facilitate authoritarian practices.These equipments are often integrated with artificial intelligence (AI) capabilities, such as facial recognition and crowd analysis. Domestically in China, they have been used for population control, monitoring dissent, and suppressing ethnic minorities, including Uyghurs in Xinjiang. If exported, these technologies could enable authoritarian regimes to implement similar practices, facilitating human rights abuses and mass surveillance, thus undermining democracy and civil liberties.

- **The United States and several European countries have restricted the use of surveillance equipment from companies like Hikvision and Dahua in critical sectors, citing national security risks.**

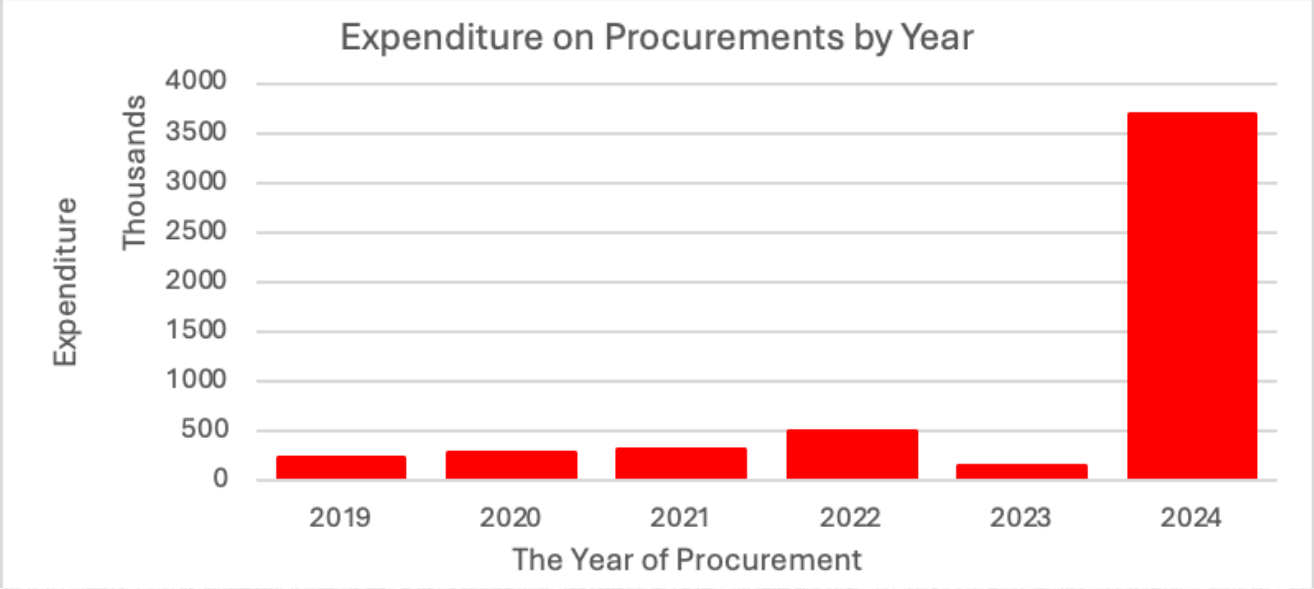
However, many developing nations have embraced Chinese surveillance technologies due to their affordability and accessibility through the Belt and Road Initiative. Despite the security risks, concerns over surveillance, and other allegations, Georgia chose PRC companies.

The United States and several European countries have restricted the use of surveillance equipment from companies like Hikvision and Dahua in critical sectors, citing national security risks. However, many developing nations have embraced Chinese surveillance technologies due to their affordability and accessibility through the Belt and Road Initiative. Despite the security risks, concerns over surveillance and other issues, Georgia chose PRC companies.

Chinese Surveillance Technology in Georgia

On December 20, **US-sanctioned** Minister Gomelauri **met** with Zhou Qian, the PRC ambassador to Georgia. During the meeting, both parties agreed on "the essence of strengthening cooperation in the field of law enforcement." The Ministry of Internal Affairs' key term was "strengthening," suggesting that these relations are already established and that efforts are being made to deepen and intensify them further.

Based on the publicly available information, Civic IDEA has investigated Georgia's procurement of surveillance cameras manufactured by Chinese companies over the past five years. The data analysis highlights a growing trend in the acquisition of Chinese technologies during this period.



For instance, in 2023, six procurements totaled 151,592 GEL. This figure surged significantly in 2024, with 13 procurements exceeding 2 million GEL.

Notably, the primary purchasers of Chinese surveillance cameras in the Georgian market comprise local self-government bodies, ministries and their subordinate organizations, educational institutions, and other entities. As for the manufacturers, some are Chinese companies involved in multiple international controversies and reputational issues, including:

Zhejiang Dahua Vision Technology Co., Ltd.,

Hangzhou Hikvision Digital Technology Co.,Ltd

Tiandy Technologies Co., Ltd.

Additionally, it is essential to highlight that out of the 46 procurements made between 2019 and 2024, 26 instances involved cameras procured by Georgian institutions manufactured by Hikvision.

The import of products from this Chinese company **has been banned** in several countries. Specifically:

In 2021, the South Korean government **imposed** a one-year ban on certain products from Hikvision. Additionally, in response to actions taken by several Western nations against Hikvision, the South Korean government removed over 1,300 Chinese-made surveillance cameras from military bases in 2024.

In 2021, the European Parliament **decided** to remove surveillance cameras manufactured by Hikvision, citing the company's involvement in human rights abuses as the primary reason for the decision.

In 2022, New Zealand's Ministry of Business, Innovation and Employment **announced** that it would no longer accept equipment from Hikvision, citing the company's involvement in human rights abuses as justification for the decision.

In 2022, the Federal Communications Commission (FCC) **prohibited** the importation and sale of video surveillance and telecommunications equipment produced by Hikvision in the US. The ban was justified by concerns over national security risks associated with the company's products.

In 2023, the National Agency on Corruption Prevention **added** Hikvision to its list of international war sponsors, citing the company's active engagement with the Russian Federation as the basis for the decision.

In 2023, Australia's Department of Defence **decided** to remove Chinese-made surveillance cameras from various government facilities, citing national security risks as the primary rationale for the decision

In December 2023, the Canadian government **decided** to ban technology produced by Hikvision, citing security risks as the justification for the decision.

In accordance with a **decision** by the United Kingdom government, all Hikvision-made cameras will be removed from sensitive government buildings by April 2025. The decision was prompted by concerns over national security risks, particularly the involvement of individuals connected to PRC in espionage activities.

In 2024, the Indian government **banned** 17 Chinese companies, including Hikvision, from participating in tenders in the country. Additionally, the government issued a warning to private companies doing business with government entities, advising them against using products from these Chinese companies.

Procurement of Chinese Surveillance Cameras by Government Entities

Table #1

Procurer	Spending
The Central Election Commission of Georgia	1,709,212
The Autonomous Republic of Adjara	1,466,841
Local government bodies (Regions)	693,328
Tbilisi	436,187
Educational Institutions	318,608
State-owned Limited Liability Companies	294,179
Ministries and their agencies	252,390
Medical Institutions	203,149
In total	**5,373,894**

As shown in **Table #1**, more than 5 million GEL was allocated to procure Chinese surveillance technology between 2019 and 2024. The Central Election Commission of Georgia was the largest purchaser of Chinese-made monitoring equipment during this period.

Notably, in 2024, ahead of the parliamentary elections in October, the Commission acquired cameras from Xiamen Milesight Technology Co., Ltd., totaling 1,694,368 GEL.

At the regional level, **local self-government bodies accounted for more purchases between 2019 and 2024 than those made directly by central government entities, such as ministries.** Key purchasers included the Shuakhevi Municipality, Zestaponi Municipality, Martvili Municipality City Hall, Tskaltubo Municipality, and Kutaisi City Hall. Notably, a substantial proportion of these purchases occurred in 2024. Namely;

- In 2024, the Zestaponi Municipality purchased 83 surveillance cameras manufactured by Xiamen Milesight IoT Co., Ltd. for 281,370 GEL.
- In 2024, the Shuakhevi Municipality purchased seven recording devices manufactured by the Chinese company Hikvision, totaling 59,000 GEL.
- In 2024, the Martvili Municipality City Hall purchased eight outdoor network cameras manufactured by Dahua.

Within Tbilisi, purchases were made in 2019, 2020, and 2024 by the Tbilisi City Assembly, the Samgori District Administration, the Didube District Administration, and the Tbilisi City Hall itself. Specifically:

- In 2019, Tbilisi City Hall spent 159,800 GEL to purchase cameras manufactured by Hikvision.
- In the same year, the Didube District Administration of Tbilisi purchased cameras valued at 20,762 GEL.
- In the same year, the Didube District Administration of Tbilisi acquired cameras worth 20,762 GEL.
- In 2024, the most recent similar purchase in the capital was made by the Tbilisi City Assembly, which acquired surveillance cameras valued at 25,150 GEL, manufactured by Xiamen Milesight IoT Co., Ltd.

After Tbilisi City Hall and local governments, educational institutions are the next largest purchasers of Chinese surveillance cameras. These include the LEPL Vocational Training Center "Lakada," LEPL Batumi Public School #10, Batumi Shota Rustaveli State University, LEPL General Giorgi Kvinitadze Cadet Military Lyceum, College Phasis, Batumi Public School #3, and LEPL Ilia Tsinamdzgvrishvili College.

Among these, the LEPL Vocational Training Center "Lakada" is particularly noteworthy, having purchased cameras and necessary equipment worth 75,611 GEL in 2024, marking the most significant purchase by an educational institution in the past five years.

Regarding Georgian companies, LLC Gardabani Thermal Power Station 2 [1] leads in purchasing Chinese surveillance cameras, having acquired cameras worth 180,588 GEL in 2022. Additionally, notable purchases have been made by companies such as Eco Service Group LLC,[2] Batumi Water Company,[3] and Georgian Gas Transportation Company LLC. [4]

Table #2

Purchaser	Spending
LEPL Common Courts Department Under High Council of Justice	182,381
Department of Environmental Supervision	22,220
Agency of Protected Areas	17,113
LEPL Labour Inspection Service	13,274
LEPL National Wine Agency	8,596
Ministry of Defence	1,316
Total	**244,900**

The largest purchaser of Chinese surveillance technology among the ministries and sub-agencies is **the Department of Common Courts under the High Council of Justice,** which carried out such procurements in 2021, 2022, and 2023. Tiandy Technologies Co., Ltd and Hikvision primarily manufacture the cameras acquired by the department. Considering the international controversies and security concerns surrounding Chinese surveillance cameras, **the purchases made by critical state agencies like the Prosecutor's Office of Georgia and the Ministry of Defense are particularly alarming.**

In 2024, the Georgian Ministry of Defense purchased Hikvision recorders. However, this is not the only instance in which the Ministry has procured surveillance equipment. Between 2019 and 2024, the Ministry initiated two electronic procedures for acquiring video technologies. Interestingly, the contracts were classified as secret in both cases, raising reasonable suspicion that the Ministry may have once again procured Chinese products. Specifically,

[1] The company is fully owned by JSC Georgian Oil and Gas Corporation, which is entirely state-owned.
[2] The company is wholly owned by the Tbilisi Municipality.
[3] The company is wholly owned by the Batumi Municipality.
[4] The company is entirely state-owned.

- In 2019, the Ministry of Defense launched a procurement process for video equipment valued at approximately 624,000 GEL. Four Georgian companies initially expressed interest, but only two—Delta Consulting LLC (397,000 GEL) and Solasi LLC (396,900 GEL)—submitted bids in the final round.

- In 2024, the Ministry initiated an electronic procurement process for video cameras valued at approximately 5,289 GEL. Among the bidders, EL + LLC and Neotech expressed interest, with the Ministry ultimately awarding the contract to Neotech for 5,100 GEL.

Notably, Neotech is a major supplier of Chinese surveillance cameras in the Georgian market. Between 2019 and 2024, the company won 13 out of 46 procurement contracts for such technology. This raises reasonable suspicion that the cameras the Ministry purchased through Neotech in 2024 were also of Chinese origin.

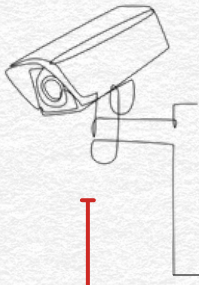
What are the risks associated with Chinese-made surveillance technologies?

Importing surveillance cameras manufactured by Chinese companies into Georgia poses significant national security risks. The challenges and vulnerabilities associated with Chinese surveillance technologies underscore these concerns.

Obligation to share information with Chinese state agencies

> ***"All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with the law, and shall protect national intelligence work secrets they are aware of. "***
>
> *Article 7, National Intelligence Law*
> *(After the amendments of April 17, 2018)*

A significant challenge associated with Chinese technology companies is **the risk of data breaches.** Under Chinese government regulations, all companies must share data with relevant state agencies when required. Of particular concern is China's National Intelligence Law (NIL), specifically **Article 7**, **which mandates that all organizations and citizens cooperate with the national intelligence services.** The international community has widely regarded this provision as a substantial risk.



- NIL applies **globally** to Chinese groups, including all subsidiaries, even those outside China. Since the Chinese parent company is subject to NIL, the law could also extend its jurisdiction to the group's foreign subsidiaries.

- NIL applies to **all organizations in China**, encompassing all types of companies established within the country, regardless of ownership—whether Chinese shareholders or foreign shareholders privately or publicly own them.

- NIL applies to **all Chinese citizens**, and as the law does not explicitly include geographical limitations, it could be interpreted to apply to Chinese citizens outside of China.

Numerous high-profile international cases demonstrate that Article 7 of China's National Intelligence Law is not merely a formal obligation however is actively enforced, with Chinese tech companies cooperating with state agencies.

For instance, a 2023 investigation by Radio Free Europe/Radio Liberty revealed that data from thousands of Chinese surveillance cameras installed in Ukraine **could be transmitted** to servers linked to the Russian Federal Security Service (FSB).

> *"Experts are confident that, when using this service, manufacturer representatives can easily access the cameras if needed. Moreover, considering the current relations between China and Russia, this could pose significant security risks"*
>
> **Serhii Denysenko**,
> Executive Director of the Computer Forensics Laboratory.

The installation of Chinese surveillance cameras in government buildings raises legitimate concerns that the Chinese government could gain access to critical state information and data through these technologies. Furthermore, based on Ukraine's experience, such information could potentially be shared with Russian federal services if deemed necessary.

Human rights concerns

As previously mentioned, Chinese tech companies often align their technological developments with the state's strategic goals to maintain support from the Communist Party. Consequently, it is not surprising that leading companies like Hikvision and Dahua play a significant role in enabling the state's repressive policies against minorities.

According to a 2019 **report** by Human Rights Watch, the Chinese government employs facial recognition technology and surveillance cameras to identify Uyghurs and monitor their movements precisely.

Authoritarian regimes can leverage Chinese surveillance technologies for similar repressive purposes. Notably, in **Uganda** and **Zambia**, state agencies reportedly used technology from a Chinese company to access data belonging to opposition political figures.

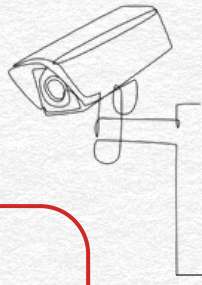
- According to **The Wall Street Journal,** Ugandan intelligence officials, with assistance from Huawei employees, hacked the WhatsApp and Skype accounts of opposition leader Bobi Wine. This allowed authorities to uncover his plans for demonstrations, leading to the arrest of the politician and dozens of his supporters.

- The Zambian government reportedly **accessed** bloggers' Facebook accounts and mobile phones to manage an opposition news website, with assistance from Huawei specialists.

Risks of Cyber-attack

International experience demonstrates that products manufactured by Chinese tech companies pose significant cybersecurity risks. Numerous studies have confirmed that Chinese surveillance systems often contain vulnerabilities that can be exploited for cyberattacks.

Cybersecurity risks are a key reason why Chinese surveillance technology is regarded as a threat to national security. For instance, in 2024, the UK **decided** to remove Chinese surveillance cameras from critical government buildings.



Ties to the Chinese Communist Party

Technology companies based in or operating in China often maintain close ties with the Chinese Communist Party (CCP). Private companies are not exempt from the party's influence, as they benefit from state subsidies and other advantages. To sustain this support, they frequently align their operations with the strategic goals of the People's Republic of China.

Additionally, shares of China's leading technology companies are often owned directly by the state or individuals with close ties to it. A notable example is Hikvision, a major manufacturer of surveillance cameras widely present in the Georgian market. As of December 2024, the state-owned Chinese company China Electronics Technology HIK Group Co., Ltd. held the largest share of Hikvision, 36.55%.

Consequently, importing Chinese technologies raises significant concerns about citizens' freedoms, as it risks “importing” Beijing’s police control practices.