THE ADVANCE OF CHINESE TECHNOLOGY

Threats stemming from Chinese technology are now making their way into people's bedrooms and garages through Lidar systems.

China's Global AI Governance Initiative is yet another example of building an anti-Western Chinese ecosystem.

The spread of Chinese technology into critical infrastructure, such as energy grids, poses a threat to Estonia's security.

China is building an integrated political and technological ecosystem based on its own standards and an amalgamation of solutions from various Chinese technology companies. A decade ago, discussions about the "export" of Chinese standards and deliberate efforts to establish dependency were already occurring within China. These discussions were accompanied by academic debates published in think tank publications, readily available in China's major bookstores. Meanwhile, the average Western individual still perceives the Chinese technological landscape as abstract and distant, failing to recognise its potential as a threat. Nonetheless, over the past decade, China has systematically wielded influence within international technical committees to champion the advancement of standards that favour Chinese technology.

The rise and global proliferation of Chinese technology is part of China's strategic efforts to enhance its political influence

The rise and global proliferation of Chinese technology are not solely the result of Chinese talents' diligence and entrepreneurship; it is part of China's strategic efforts to enhance its political influence alongside exporting its standards. China aims to reach a point where integrated technological solutions cannot be replaced by Western technology due to both incompatibility and deep interconnection.

The Chinese Communist Party's (CCP) deliberate drive to undermine Western influence and move towards a "democratic" multipolar world order, accommodating the principles and interests of authoritarian regimes, further reinforces the CCP's determination to create an ecosystem independent of the West. The clearest manifestation of this is the Belt and Road Initiative, along with the Digital Silk Road. Similarly, the Global Artificial Intelligence (AI) Governance Initiative introduced by Xi Jinping during the Belt and Road Summit in October is another example of China's efforts to build an anti-Western ecosystem.

State-owned Chinese enterprises are highly likely to have much easier access to capital than ordinary Chinese businesses.

Both the public and private sectors should take forward-looking measures to prevent the proliferation of Chinese technology, as it is highly likely that, in the not-so-distant future, a painful decision to abandon Chinese technology may be necessary due to geopolitical developments and security concerns. This decision is made more painful by the fact that Chinese companies offer products and services at more affordable prices to foster dependence. This approach often appears efficient for both private enterprises and the public sector, where the principle “cheapest wins” often applies in government procurement.

Over the past year, we have witnessed how Chinese technology is penetrating an entirely new area in Estonia – the electrical grid. After being excluded from 5G networks, Huawei has targeted cloud services and solar and wind farms. Both Huawei and other Chinese companies seek to supply Estonian electricity networks with inverters and energy storage systems connecting solar and wind farms to the national grid.

An inverter is a device that converts electricity generated by solar panels into usable energy for consumers. Inverters are connected to the internet for managing and monitoring solar power plants, allowing remote control and adjustment of parameters and power. Like other electronic devices, inverters require software updates and adherence to the manufacturer’s recommendations. However, providers of products with critical functions must be trusted not to manipulate the device and, consequently, the critical service it provides. The more Estonia relies on solar farms for its power generation, the more significant the impact such manipulation could have on the country’s electricity production capacity. It is, therefore, essential to avoid a situation where a third party can exploit the country’s electricity supply for intelligence gathering or exert economic and political pressure.

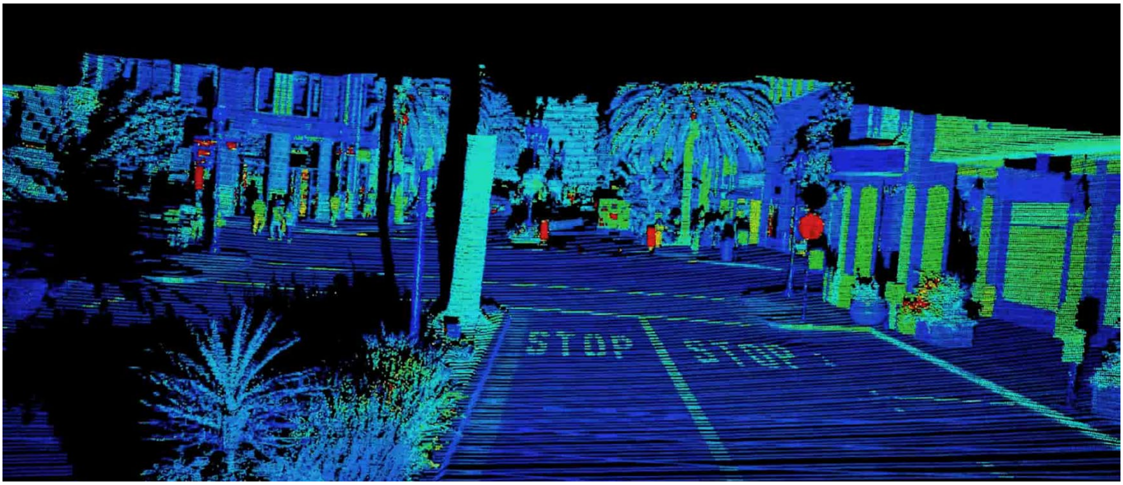
The introduction of Chinese inverters and energy storage systems into Estonian electricity networks could lead to a repetition of the 5G scenario sooner or later. Both the business sector and the government must be acutely aware of the implications of introducing Chinese technology into Estonia’s critical infrastructure. Huawei’s work in Estonia is persistent, comprehensive and systematic, and it is coordinated with its headquarters in Shenzhen.

A significant challenge with Chinese technology companies is their potential state affiliation.

A significant challenge with Chinese technology companies is their potential state affiliation. China increasingly conceals company background information, citing data security concerns to limit transferring specific data beyond its borders. In recent years, Chinese authorities have imposed several new restrictions on disclosing information about Chinese companies.

A new wave of threats stemming from Chinese technology is marked by the ever-wider adoption of Lidar systems, from household electronics to self-driving cars. These devices use Lidar systems to scan their surroundings for independent operation. In addition to surfaces, they also scan objects to detect potential hazards behind them. For example, self-driving cars must assess whether a ball could roll onto the road behind a parked car or a child might move in that direction, requiring the parked car to be scanned.

We have credible information about a Chinese manufacturer working on Lidar systems for self-driving cars that are intended to scan the car's entire surroundings and transmit the information to a database in China. While a device collecting data for autonomous operation should delete any non-essential data, this Chinese company aims to transfer the complete environmental data to a Chinese database. This raises concerns that Chinese technology-enabled self-driving cars could be vulnerable to exploitation for intelligence purposes.



Surroundings scanned with Lidar technology.

Source: seyond.com

A similar threat also applies to ordinary household electronics, such as robot vacuum cleaners, which scan their entire environment. Furthermore, there is a risk that personalised services offered by Chinese technology companies, combined with accounts for mobile applications, collect information about consumers based on their behaviour.

Next, attention should be turned to the Chinese video hosting service TikTok and its owner, ByteDance. TikTok is a classic example of combining an obscure background and data collection for the purpose of developing new capabilities. While TikTok's parent company, ByteDance, is registered in the Cayman Islands, its actual headquarters are in Beijing, where ByteDance has registered another entity, Douyin Co., Ltd. However, Douyin, with no employees, essentially serves as a shell company for the Cayman Islands-registered entity.

Douyin Co., Ltd., in turn, owns Beijing Douyin Information Service Co., Ltd., which has 1,947 employees and serves as ByteDance's actual headquarters. Located in the AVIC Plaza building in the Haidian district of Beijing, this subsidiary maintains a complex ownership structure, with a 1% stake held by the National Computer Network Emergency Response Technical Team/Coordination Centre of China (CNCERT/CC), a Chinese state entity. CNCERT/CC operates under the Central Cyberspace Affairs Commission, which answers to the CCP Central Committee. The Central Cyberspace Affairs Commission formulates and executes China's cyberspace policies and decisions. This arrangement raises questions regarding the significance of the 1% ownership stake.

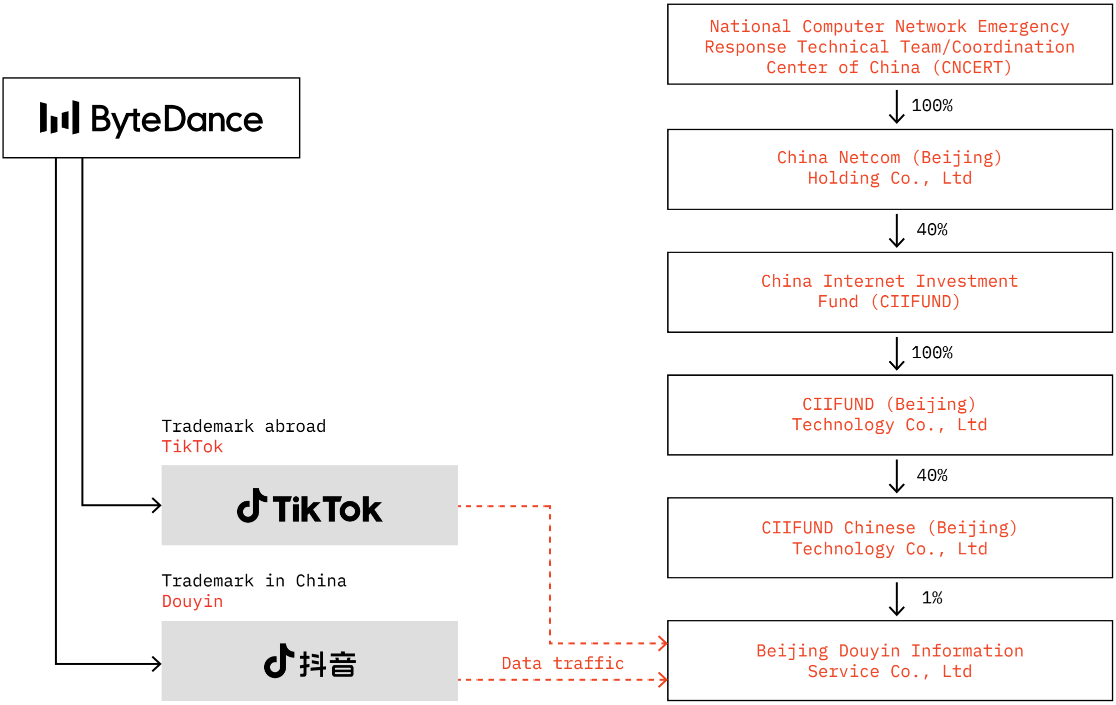
During a US Congress inquiry into TikTok on 23 March 2023, TikTok's CEO, Shou Zi Chew, explicitly confirmed that data gathered worldwide via the TikTok video app is currently sent directly to Beijing Douyin Information Service in China. This also applies to data collected via the Douyin app inside China. The implication is that CNCERT/CC has access to data collected both within China through Douyin and internationally through TikTok.

The massive collection of data provides ByteDance with the opportunity to develop artificial intelligence.

The massive collection of data provides ByteDance with the opportunity to develop artificial intelligence. China needs access to visual and behavioural data from people of various origins to develop globally competent artificial intelligence. Data collected solely from China would not offer such an opportunity because the appearance and behavioural patterns of people in China significantly differ from those in many other parts of the world.

In addition to the development of artificial intelligence, the data collected by the application may also be useful for other purposes. TikTok extensively gathers information about the device and its user, including contacts, calendars, other applications, Wi-Fi connections and location. Such information can be valuable for intelligence gathering, extortion and cyberattacks, as it can be used to craft convincing phishing emails tailored to a specific individual or their employer. This is especially concerning when the user's employer is an institution or company that could be of strategic interest to China.

In addition to TikTok, Douyin Co., Ltd also owns an entity and brand called Toutiao. Both Toutiao and Beijing Douyin Information Service share the same legal representative. This implies a close connection between TikTok and Toutiao. Toutiao's unique feature in the Chinese market is that it offers personalised news feeds developed by artificial intelligence based on user behaviour patterns. Essentially, using TikTok means assisting a company with ties to an authoritarian state, which aims to reshape Western security architecture, in developing artificial intelligence.


National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT)
100%
China Netcom (Beijing) Holding Co., Ltd
40%
China Internet Investment Fund (CIIFUND)
100%
CIIFUND (Beijing) Technology Co., Ltd
40%
CIIFUND Chinese (Beijing) Technology Co., Ltd
1%
Beijing Douyin Information Service Co., Ltd
ByteDance
Trademark abroad
TikTok
TikTok
Trademark in China
Douyin
抖音
Data traffic

The TikTok ownership scheme.