Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: The Editorial Board

Huawei at the centre of Spanish security—will Madrid pay the price of trust?

On 11 July, the Ministry of the Interior of Spain signed a contract worth 12.3 million euros with Huawei for the maintenance and management of the data collected by the SITEL system, the national mechanism for lawful interception of communications.

The procurement process was carried out via the Plataforma de Contratación del Sector Público, the Spanish government's official electronic system for all public tenders.

Huawei was awarded the contract because it was estimated to be the most favourable company, according to the overall criteria of its economic offer and technical capacity.

Although this decision does not formally go beyond the scope of the standard public procurement procedure, its political and security weight far exceeds the administrative limits of the tender.

SITEL (Sistema Integrado de Interceptación de Telecomunicaciones) is an important platform through which the Spanish security authorities intercept and archive, on the basis of court orders, the communications of persons who are reasonably suspected of being linked to terrorism, organised crime, or serious crimes. Police and intelligence services' work relies on the management and maintenance of such systems.

Therefore, the decision to entrust this task to a Chinese company has raised complex issues of strategic trust.

National security vs foreign tech

Huawei is a tech giant that is obliged under China's 2017 National Intelligence Law to support national security activities at the request of its government agencies.

The company points out that it operates in accordance with the laws of each country in which it has contracts and that it has never shared data with Chinese authorities beyond local regulations.

However, the nature of China's political system and the broad interpretation of security interests within PRC legislation open up the dilemma of the extent to which Huawei could refuse Beijing's possible request if it were formally made through the national security mechanisms.

Most importantly, this issue has already met with a reaction in professional security circles in Spain itself.

The analyses published by the portal The Record (Recorded Future), which specialises in national and cyber security, indicate that the Spanish National Police and the Civil Guard have raised objections about the risk of potentially compromising confidential data.

> Such contracts can create long-term structural weaknesses in terms of data protection that could potentially be exploited in a different political environment

These statements indicate that some experts consider this type of contract with Huawei to be risky, as in the event of a serious political confrontation between the West and China, there is a possibility that the data stored on Huawei's servers could become the object of interest of the Chinese intelligence services, even though the physical storage of the data is under the control of Madrid.

It was said that there is "growing concern" among high-ranking officials of the National Police and the Civil Guard about the role of the Chinese provider in the system that processes the most sensitive data from criminal investigations and counter-terrorism operations.

It was also highlighted that some experts in the Spanish intelligence community believe that such contracts can create long-term structural weaknesses in terms of data protection that could potentially be exploited in a different political environment.

Experts warn of realistic compromise scenarios

Despite claims that Spain has complete control over the encryption keys, security experts in Europe point to several realistic compromise scenarios.

The first risk concerns the so-called firmware and software backdoors, which allow the device manufacturer to maintain the possibility of remote access for maintenance or emergency operations.

Firmware is a special type of software that is built directly into electronic devices and controls the basic functions of their hardware. It can be said to be the layer between the physical components and the operating system or applications. If such a channel existed, it could be used in an emergency situation to obtain metadata or even partial communication content.

Another risk lies in the supply chain for spare parts and upgrades, where subtle changes to hardware or microcode can form the basis for subsequent data capture. A particular challenge is the possibility that, even without directly cracking the encryption, a sophisticated analysis of traffic and access patterns allows the construction of a network environment that reveals patterns of police and intelligence work.

> Information security experts point out that physical and software access to devices remains a vendor-dependent segment

Technically, the contract provides for the use of Huawei OceanStor 6800 V5 server units to store the interception logs. These systems enable high capacity, rapid processing, and data storage with backup copies.

The Centro Criptológico Nacional, an institution that sets cryptographic standards for all security and administrative authorities in Spain, will supervise encryption and certification.

Government sources who have commented on the details of the contract state that the key to decrypt the data is exclusively in the hands of the domestic institutions. However, information security experts point out that physical and software access to devices remains a vendor-dependent segment, which always leaves room for potential pressure.

Huawei as a "high-risk supplier"

The context in which this contract was concluded makes it an additional object of attention. In recent years, the European Commission has adopted recommendations in which it advises its members to limit the participation of suppliers from countries whose legal and political framework may require cooperation with intelligence structures in critical infrastructure projects.

Although Huawei is not officially banned in these documents, the company is categorised as a "high-risk supplier" whose equipment is not recommended for use in state security systems without specific national protection mechanisms.

Poland, the Netherlands, Denmark, and the Baltic states have already issued internal regulations that almost completely exclude Huawei from strategic telecommunications projects.

The United Kingdom and the United States have gone a step further and implemented practical bans on Huawei in all sensitive areas of their national and federal networks.

Experts within NATO's cybersecurity coordination structures suggest standardising regular reviews at the alliance level in such situations. The idea of introducing joint reviews of devices and software systems, which have been proposed in several internal memoranda of the NATO Defence Policy and Planning Committee, is gaining momentum.

> The lobbying element further fuels the debate on whether economic and political pressure influences security decisions

At the European Union level, there are also increasing proposals for the establishment of a permanent independent body that would carry out technical and legal due diligence analyses of contracts involving the infrastructure of suppliers outside the EU or countries with robust data protection systems.

This would significantly reduce the possibility of individual members, driven solely by short-term financial interests, jeopardising collective security standards.

The Spanish government under the leadership of Pedro Sánchez has intensively expanded economic relations with China in recent years, including through projects in the areas of transport, smart cities, and energy.

According to reports, Huawei has engaged local lobbying firms in Spain to mitigate the resistance encountered during the tender preparation by establishing connections with political entities and research institutions.

Although everything was done within the framework of Spanish laws on the transparency of lobbying, this element further fuels the debate on whether economic and political pressure influences security decisions, which ideally should be purely professional and strategic.

Balancing security and sovereignty

Looking to the future, two scenarios are possible. If the implementation of the Huawei solution proves to be without technical problems, data leaks, or security threats, Spain will be able to present this contract as an example of how, with strict domestic controls, the technology of a provider that is subject to restrictions in other countries can be exploited.

This would allow Madrid to win the argument that it combines economic benefits with security requirements, especially if it proves this through savings compared to competing offers.

The most significant challenge for these agreements arises during times of crisis, when geopolitics supersedes all economic and technical assurances - Wang Yi with Ursula von der Leyen

However, the most significant challenge for these agreements arises during times of crisis, when geopolitics supersedes all economic and technical assurances.

Should relations between the West and China enter a phase of deep strategic conflict tomorrow, the issue of access to sensitive databases could become a pressure point in negotiations and political blackmail. In such circumstances, even the strictest technical protocol barriers do not guarantee complete resistance.

Therefore, more and more experts within NATO and the EU believe that areas of data processing and storage that are important for security and sovereignty should remain under full national control, even if this means higher costs for national budgets.

The second scenario implies that in the event of a data leak, a cyber incident, or even a serious suspicion of compromise, the consequences would be much more far-reaching.

Spain could then face not only a domestic

political crisis but also a revision of relations within NATO and the EU when it comes to joint intelligence cooperation projects.

The allies could demand additional technical reviews or even temporarily restrict the sharing of classified information until the system's level of vulnerability is determined.

In any case, this tender shows how a simple administrative procedure, such as the tendering and awarding of contracts for IT services, can in reality raise complex issues that go to the heart of international relations and strategic trust.

In the coming period, Spain will have to prove to its citizens and partners that economic profitability was not more important than security and that control over the most sensitive areas of state power lies exclusively in the hands of its institutions.