Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

Spain's deal with Huawei raises security questions within NATO and the EU

When the Ministry of the Interior of Spain signed a contract worth 12.3 million euros with the Chinese company Huawei on 11 July, it appeared to be a routine public procurement task.

The contract provides for Huawei to manage and maintain the storage of data collected via SITEL—the national system for telecommunications interception used by the Spanish police and intelligence services.

However, just two days later, Tomorrow's Affairs warned in the article "Huawei at the centre of Spanish security—will Madrid pay the price of trust?" that this is not a technical matter but a serious security precedent.

On 13 July, our portal published a detailed analysis that clearly points out the strategic risks that such a contract entails.

These include the possibility of unauthorised access to metadata, technical vulnerabilities arising from the architecture of the Huawei servers themselves, and the deep mistrust that such a move could cause among Spain's allies in NATO and the European Union.

We have pointed out that although the physical infrastructure is under the control of Madrid and the encryption keys are in the hands of domestic institutions, the existence of the so-called "software and firmware layers", which are fully controlled by the manufacturer, opens up room for potential manipulation and compromise of the system—in moments of crisis, without any warning.

It is even more important to emphasise that, despite the supposed isolation of the system, sensitive parts of SITEL—such as interception logistics and access protocols—rely on continuous technical support. Any disruption to the support chain or confidence in the reliability of the supplier has a direct impact on the operation of the system.

At a time when global security standards are increasingly reliant on continuous and transparent functionality, this type of contract creates an imbalance that can have practical consequences in crisis situations.

Neither premature nor exaggerated

In the days that followed, it became clear that these warnings were neither premature nor exaggerated. The reaction in Washington was almost immediate.

Congressman Rick Crawford said that Spain was threatening its own security as well as the security of its allies. Along with Senator Tom Cotton, he sent a letter to the Director of National Intelligence, Tulsi Gabbard, asking that the sharing of classified information with Madrid be temporarily suspended until the security implications of the deal are fully assessed.

Our portal has announced this as a possibility, i.e., a consequence, in the 13 July article.

There was also a reaction in Brussels. European Parliament MEPs expressed their surprise that an EU member state had entrusted a Chinese company with sensitive security tasks despite official recommendations from the European Commission to minimise the use of equipment from "high-risk suppliers."

> Huawei is legally obliged to cooperate with the intelligence structures of the People's Republic of China when requested to do so

The analysis by an organisation specialising in digital rights, ARTICLE 19, pointed out that under the 2017 Chinese National Intelligence Law, Huawei is legally obliged to cooperate with the intelligence structures of the People's Republic of China when requested to do so, as we also pointed out and warned in the article.

Independent cyber analysts believe that even a firmware version reinforced with security

measures can contain latent mechanisms that are later activated—either by remote updates or by physical changes to servers during an overhaul.

This approach is considered critical enough in real-world security tests, and the system is not considered "closed" solely due to key encryption.

This is confirmed by reference to similar cases of security vulnerabilities in other countries, where "invisible" access levels were only discovered after a detailed, independent audit.

Not what Huawei formally is, but what it could become

On paper, Huawei complies with the laws of every country in which it has contracts. The company itself also claims this—it states that it has never passed on data to the Chinese authorities that goes beyond the legal framework of the country in which it operates.

However, the political and security problem is not what Huawei formally is, but what it could become in the event of a major political conflict between the West and China.

This is why not only American and European officials but also Spanish security institutions are concerned.

According to the information we have published, there is growing concern among the National Police and the Civil Guard that the technical management of the sensitive system is being entrusted to a company from a country whose legislative and political system allows cooperation with the secret services without a court order.

> Even without direct access to the content, compromising the functioning of the system can cause significant disruption to security and strategy

Their concern is not only about the possibility of direct wiretapping but also about more sophisticated methods—such as analysing network patterns, monitoring access points, data processing plans, and the dynamics of intelligence operations. Such patterns can reveal the internal logic of the security apparatus, even without insight into the specific content of the communication.

Digital forensics experts point out that analysing metadata can reveal the structure of networks, identify central figures in operations, and identify temporal patterns that reveal the early stages of investigations.

This means that even without direct access to the content, compromising the functioning of the system can cause significant disruption to security and strategy.

Changing the nature of alliances

The government of Pedro Sánchez defends the contract. It claims that everything has been carried out in accordance with the law, that the systems are isolated and certified, and that there is no technical possibility that the data can be compromised.

The Spanish institution responsible for cryptological standards has also technically confirmed the contract. The government argues that Huawei does not manage the wiretaps but only maintains the infrastructure and that the Spanish institutions have full control over the system at all times.

Contracts involving critical information systems must be

subject to the highest levels of oversight, institutional accountability, and strategic assessment of long-term consequences

However, there are indications from diplomatic circles in Brussels that this case could be the trigger for the establishment of a body to oversee such policies if a coordinated European position on the independent assessment of critical technology contracts is not established.

This would mean that a member state could not unilaterally sign collective defence contracts without the consent of the other states.

In the modern world, where digital infrastructure is a central point of strategic stability, the question of who manages the servers is no longer just a technical issue but a deeply political one.

The Spanish case shows that fictitious administrative efficiency and savings can come at a high price—both in terms of security integrity and international trust.

Decisions that are formally considered commercial increasingly have consequences that change the nature of alliances.

Therefore, contracts involving critical information systems must be subject to the highest levels of oversight, institutional accountability, and strategic assessment of long-term consequences.