Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

China's ongoing cyber campaign against Taiwan

In early January, Taiwan's National Security Bureau (NSB) released its annual analysis of the cyber threats the island faced in the previous year.

The document bears a clear title: "Analysis of China's Cyber Threats to Taiwan's Critical Infrastructure in 2025." The document explicitly identifies the source of the threat. Taiwanese authorities directly attribute the pressure to China.

The document states that in 2025, an average of 2.63 million unauthorised access attempts per day were recorded, targeting systems deemed essential to the functioning of the state.

Compared to 2024, when the average was about 2.46 million per day, this represents a continuation of the growth observed in previous years. As recently as 2023, the figure was almost half that amount.

These figures alone do not constitute evidence of massive breaches or system collapse. The National Security Bureau emphasises that these are attempts, not confirmed intrusions.

However, their political and security significance lies not in individual incidents, but in their continuity. When such pressure becomes routine and long-term, it ceases to be an extraordinary event and begins to influence how the state plans, invests, and makes decisions.

Critical infrastructure under pressure

Critical infrastructure, as defined by Taiwan, includes sectors without which modern society cannot function. These are public administration, energy systems, communications and data transmission, transport, health facilities and emergency services, water supply, the financial system, and large industrial and technological complexes.

Domestic media reports from 2025 indicate that unauthorised access attempts repeatedly targeted all these sectors.

The energy sector is particularly notable. The National Security Bureau reports that efforts targeting energy infrastructure in 2025 have increased manifold compared to the previous year.

> The analysis notes that in 2025, at least twenty cases were identified in which hospitals were exposed to ransomware attacks

Energy systems underpin almost all other sectors of society. Disruption in this area has a cascading effect, impacting everything from communications to hospital operations.

Even without an actual supply disruption, this mere possibility necessitates the constant mobilisation of resources and attention.

The health system is another area under significant pressure. The analysis notes that in 2025, at least twenty cases were identified in which hospitals were exposed to ransomware attacks – attempts to block information systems to extort or destabilise operations.

Such attacks do not always involve financial demands. Simply disrupting hospital operations is enough to create pressure on the administration and a sense of insecurity in society.

Supply chains: the weakest link

The methods used are not spectacular, one-off operations, but rather a combination of technical and organisational approaches.

The most common tactics include exploiting known vulnerabilities in hardware and software, overloading networks to render them unavailable, deceiving employees to obtain access credentials, and attacking through suppliers and partners.

Large institutions – ministries, energy companies, hospitals – have dozens or hundreds of outsourcers: IT firms maintaining software, companies managing servers, equipment manufacturers, billing firms, logistics providers, and even outsourced email or monitoring services.

These partners require constant digital access to the client's systems to perform their work.

> Attackers target a smaller firm in the supply chain, which has weaker security, fewer staff, and often less robust access controls

An attacker does not attempt to breach the most heavily protected system directly. Instead, they target a smaller firm in the supply chain, which has weaker security, fewer staff, and often less robust access controls.

By compromising that service supplier, the attacker gains something far more valuable than the initial intrusion: legitimate credentials, digital certificates, or software updates that appear authentic.

Such tactics suggest long-term observation and testing of the system, depending on the inevitable mistakes that occur in large organisations.

The names behind repeated cyber operations

The analysis also identified groups associated with these activities, including BlackTech, Flax Typhoon, Mustang Panda, APT41, and UNC3886.

These names do not refer to official state institutions with a formal hierarchy or public identity. Instead, they are work labels used by security services and specialised companies to group recurring attack patterns that share the same technical characteristics, objectives, and modus operandi.

> The same tools, types of malicious code, server channels, or tactics for system entry appear in different incidents

In other words, when the same tools, types of malicious code, server channels, or tactics for system entry and persistence reappear in different incidents, those events are linked and assigned a single label.

This enables services to monitor the continuity of operations, even when specific individuals or technical details change.

Not random: cyber attacks and political timing

In Taiwan's report, these labels are used to demonstrate that the pressure is neither random nor isolated but comes from persistent actors whose activities are repeated over many years.

The National Security Bureau links them to Chinese interests but deliberately uses technical language, avoiding political labels and public accusations that cannot be precisely proven.

One of the report's more important elements is the connection between the intensity of cyber activity and the political calendar.

The National Security Bureau recorded an increase in access attempts during May, the first anniversary of President Lai Ching-te's inauguration, and in November, when Vice President Hsiao Bi-khim was in Europe.

The rise in cyber activity during politically sensitive events shows that attacks are not random - Lai Ching-te

The rise in cyber activity during politically sensitive events shows that attacks are not random. When Taiwanese officials make important decisions or act on the international stage, their intensity increases.

Such a pattern indicates that cyber pressure is being used to convey a message: that political moves have been observed, monitored, and taken into account.

Unlike military or economic measures, this approach does not require open escalation but allows for sustained pressure without formally crossing the threshold of conflict.

In this context, cyber activities cease to be merely a technical problem and become part of political pressure. They do not necessarily aim to immediately disable the system but to demonstrate the ability to disrupt and burden.

This approach shifts the balance: institutions are forced to maintain a heightened level of preparedness, which, over time, consumes resources and changes priorities.

Cyber pressure as everyday reality

The most serious consequence of this pressure is not evident in individual incidents but in how the state must allocate its resources.

When unauthorised access attempts occur daily and on a large scale, security is no longer an extraordinary issue; it becomes a permanent obligation that shapes spending, employment, and training, as well as the organisation of public services.

In this respect, Taiwan finds itself in a situation that signals a broader trend. Cyber pressure does not need to cause a dramatic collapse to have serious consequences; it is enough for it to become part of everyday life.

> In 2026, the real challenge will not be a single major breakthrough but the gradual erosion of attention, resources, and trust

Normalising pressure blurs the line between peace and conflict, and security is measured by the system's ability to function under constant stress.

In 2026, the real challenge will not be a single major breakthrough but the gradual erosion of attention, resources, and trust.

Taiwan's experience demonstrates that the key difference between resilience and vulnerability lies in management, not in the complete absence of threats. Attempts will persist. The question is whether they will remain politically significant or become an operational routine with little impact.

The report by Taiwan's National Security Bureau leaves little room for doubt. Cyber activities recorded during 2025 were continuous, targeted, and clearly directed at sectors crucial to the functioning of the state.

They were not intended to cause the immediate collapse of the system but to impose long-term strain and test its resilience.

This approach shows that cyberspace is being used as a means of pressure that does not require formal conflict yet produces lasting security and political consequences.