Analysis on China's Cyber Threats to Taiwan's Critical Infrastructure in 2025

I. Trends and developments

1. China increases cyberattacks against Taiwan year by year

Taiwan's national intelligence community identified a large number of major cybersecurity incidents in 2025. On average, China's cyber army launched 2.63 million intrusion attempts per day targeting Taiwan's critical infrastructure (CI) across nine key sectors, namely administration and agencies, energy, communications and transmission, transportation, emergency rescue and hospitals, water resources, finance, science parks and industrial parks, as well as food. This figure marks a 6% increase compared to 2024 (as shown in Figure 1). Such a trend indicates a deliberate attempt by China to compromise Taiwan's CI comprehensively and to disrupt or paralyze Taiwanese government and social functions. China's moves align with its strategic need to employ hybrid threats against Taiwan during both peacetime and wartime.

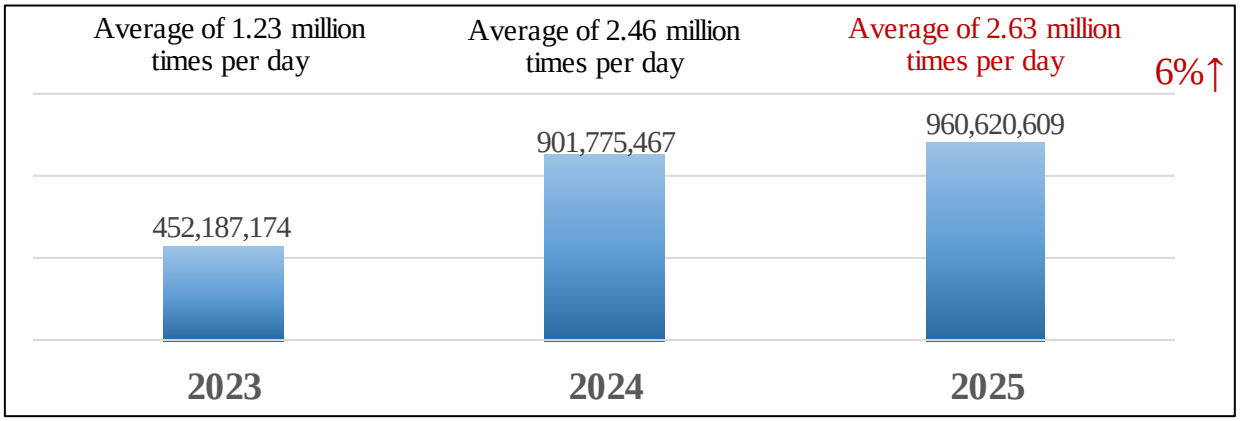

Figure 1: China's cyberattacks against Taiwan's CI from 2023 to 2025

Furthermore, compared with 2024, cyberattacks by China's cyber army against Taiwan's CI in 2025 increased most significantly in the sectors of energy as well as emergency rescue and hospitals (as shown in Figure 2).

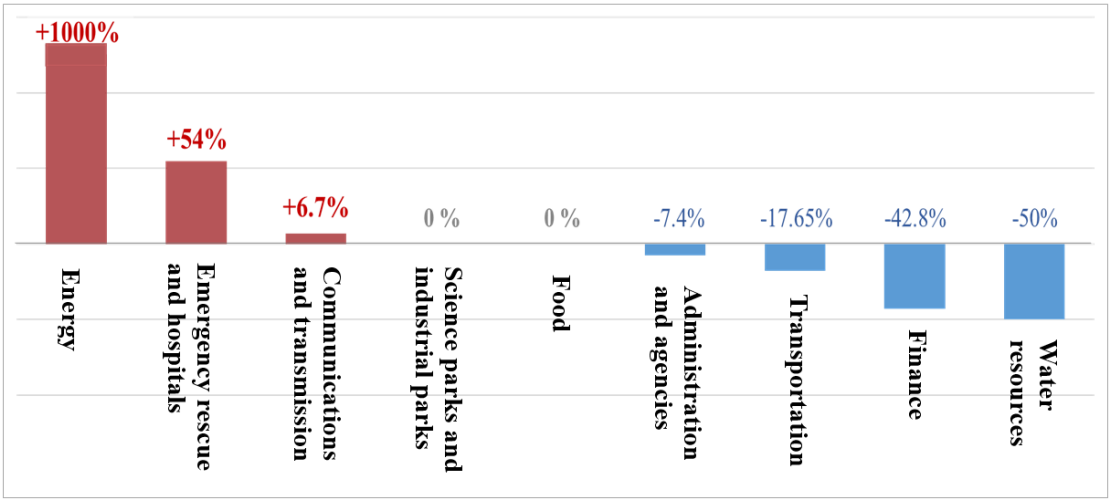

Figure 2: Statistics on the growth of China's cyberattacks against Taiwan's CI in nine sectors in 2025

2. China conducts cyber operations in conjunction with political and military coercion

China's cyberattacks targeting Taiwan exhibit the characteristics of political and military coercion. In 2025, China's cyberattacks against Taiwan demonstrated a degree of correlation with the joint combat readiness patrols (JCRP) conducted by the People's Liberation Army (PLA) against Taiwan. The PLA conducted a total of 40 JCRPs against Taiwan in 2025. During which, China's cyber army simultaneously escalated their cyberattacks against Taiwan for 23 times.

In addition, China ramped up hacking activities during Taiwan's major ceremonies, issuances of important government

statements, or overseas visits by high-level Taiwanese officials, attempting to disrupt government services and undermine people's morale. Adding to that, China launched hybrid intimidation against Taiwan with cyberattack incidents peaking in May of 2025, the first anniversary of President Lai's inauguration. (as shown in Figure 3)

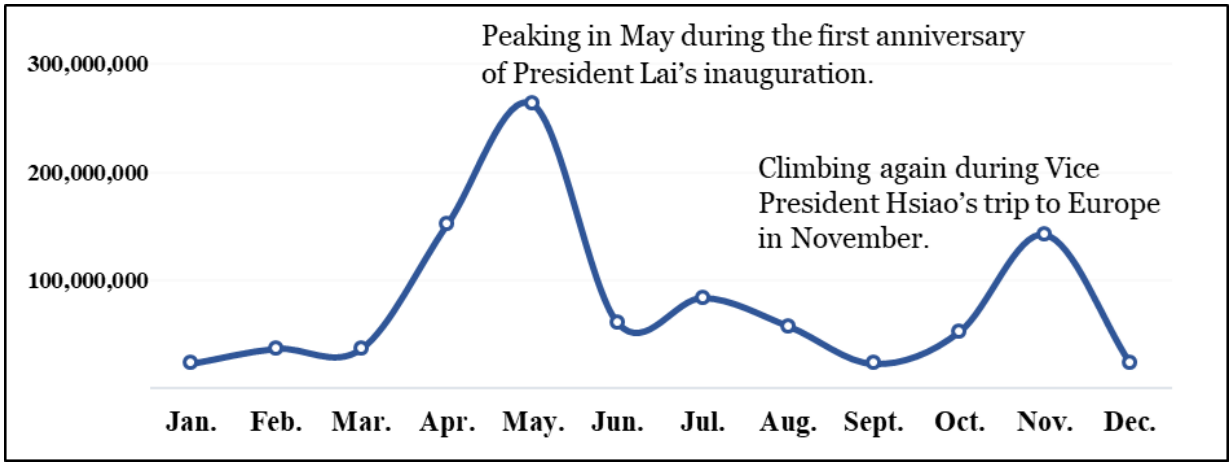

Figure 3: China's cyberattacks against Taiwan's CI in 2025

II. Hacking tactics and targets of attacks

1. Four major hacking tactics

China's cyberattacks against Taiwan's CI involve four major tactics: attacks on hardware and software vulnerabilities, distributed denial-of-service (DDoS) attacks, social engineering attacks, and supply chain attacks. China has flexibly maneuvered these tactics to launch cyberattacks.

A. Attacks on hardware and software vulnerabilities: Among all China's cyberattacks against Taiwan, over 50% cases involve attacks on hardware and software vulnerabilities (as shown in Figure 4). It can be seen that China has exploited the

vulnerabilities discovered by Chinese industries, government, and academia to strengthen the technology capacity of vulnerability weaponization. It has actively leveraged the software and hardware vulnerabilities of information communication technology (ICT) equipment manufactured by international suppliers or that involved in government procurement joint supply contracts. Chinese hackers would target ICT equipment of Taiwan's CI with unpatched vulnerabilities to circumvent identity verification and gain administrative access for secret theft.

B. DDoS attacks: China's cyber army exploits a large number of botnets to send high-frequency connection requests simultaneously with an aim to compromise the operation of CI's external networks. Such a move intends to delay or paralyze CI's services, and thus impact Taiwanese people's daily lives.

C. Social engineering attacks: China's cyber army is sophisticated in posing as business contacts of its targets and sending phishing emails to lure specific targets to click on malicious links and open malicious attached files. Chinese hackers may also employ the ClickFix technique to fabricate error messages or update requirements. These techniques aim to lure the targets to activate malware, and take the chance to acquire higher system permissions.

D. Supply chain attacks: China's cyber army also tries to infiltrate into the networks of suppliers of Taiwan's CI as well as their cooperative enterprises. Through the approach of conducting identity-theft to cover illegal activities, Chinese hackers would seize those targets' shared systems, system upgrades, and equipment maintenance to implant and spread malware among Taiwan's CI.

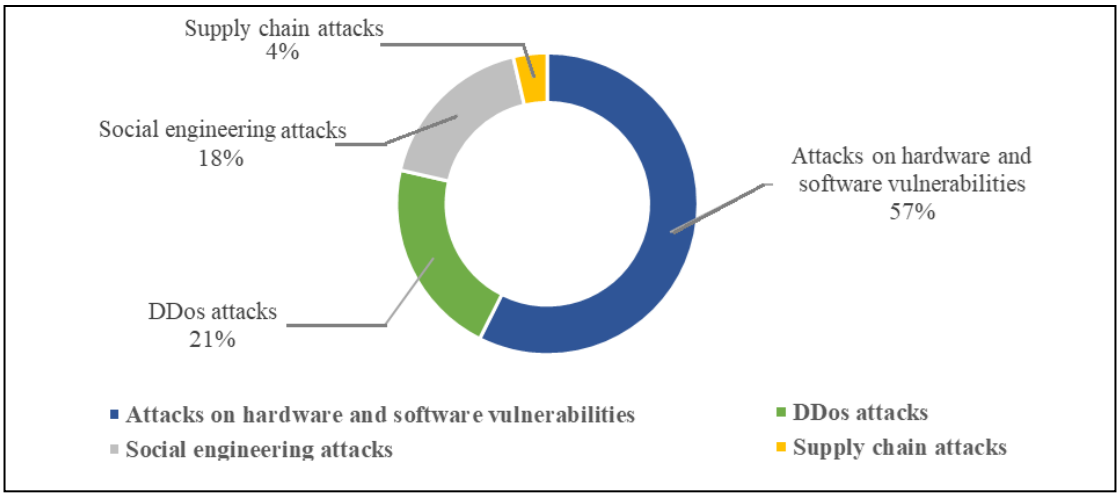

Figure 4: Distribution of China's cyber hacking tactics against Taiwan's CI in 2025

2. Five major targets: The cyber operations launched by China's cyber army against Taiwan's CI are mainly carried out by five Chinese hacker groups, including BlackTech (黑科技) (as shown in Table 1), with each hacker group targeting different CI sectors.

Hacker groups	Targeted sectors
BlackTech（黑科技）	Administration and agencies, communications and transmission, and science parks
Flax Typhoon（亞麻颱風）	Emergency rescue and hospitals, and science parks
Mustang Panda（野馬熊貓）	Administration and agencies, and energy
APT41	Administration and agencies, energy, communications and transmission, emergency rescue and hospitals, science parks, transportation, and water resources
UNC3886	Administration and agencies, and science parks

Table 1: Top five Chinese hacker groups launching cyber operations against Taiwan's CI in 2025

A. Energy sector: Infiltrating into industrial control systems to compromise the operation of energy companies

China's cyber army intensively probes into the network equipment and industrial control systems of Taiwan's public-owned and private energy companies, including those in the petroleum, electricity, and natural gas sectors. In addition, when Taiwan's energy companies carry out software upgrades, Chinese hackers would take the opportunity to implant malware into their systems, so as to keep track of the operational planning of Taiwan's energy sector concerning operational mechanisms, material procurement, and establishment of backup systems.

B. Healthcare sector: Stealing personal data for blackmail

China's cyber army continues exploiting vulnerabilities in the websites and systems of major hospitals in Taiwan, and utilizes ransomware to compromise the operation of those hospitals, or even steal information concerning patients' personal data and healthcare research results. Statistics show that Chinese hackers have sold data stolen from medical institutions on dark web forums at least 20 times in 2025. Such a move attempts to achieve multiple objectives such as collecting information, seeking profits, and intimidating Taiwan's general public.

C. Communications and transmission sector: Exploiting vulnerabilities of network systems to stay in the background

China's cyber army exploits the vulnerabilities in the network systems of Taiwan's telecommunications companies, aiming to stay in the background of the computer systems of those companies and

their contractors. In addition, China's cyber army utilizes a Man-in-the-Middle attack (an active attack where the threat actor hijacks a communication link to intercept and tamper with the communication content without the knowledge of either party) to steal their communication data and user information while penetrating their sensitive and backup communication links. Such a move could impact the security and resilience of Taiwan's domestic and international telecommunications networks.

D. Administration and agencies: Conducting attacks tailored to latest political events

China's cyber army targets specific departments of Taiwan's central government with tailored social engineering emails, posing as individuals sending business correspondence or offering reports on international trade and cross-strait affairs. As these emails contain malware in the attachments, targets would be lured to click on the attachment and implant backdoors for data theft. Additionally, after stealing the targeted information, Chinese hackers would process and rewrite it to disseminate on the dark web and specific forums. China's moves aim to gather intelligence on Taiwan's government and undermine public trust in the government's cybersecurity capabilities.

E. Technology sector: Targeting chip and military technologies

In addition to attacks targeting Taiwan's science parks, China's cyber army also hacks into semiconductor and military industries, spanning from upstream, midstream, and downstream companies involved in design, manufacturing, and packaging and testing. In particular, it would utilize diverse tactics such as supply chain

attacks, social engineering emails, and vulnerability exploitation to steal advanced technologies, industrial plans, and decision-making intelligence, in an attempt to support China's self-reliance in technology and economic development and prevent China from being put in a disadvantage position in the US-China technology competition.

III. Conclusion:

Since 2025, cybersecurity agencies and intelligence services across the Indo-Pacific region, NATO, and the European Union have repeatedly identified China as a primary source of global cybersecurity threats. (as shown in Table 2)

Dates	**Countries/Organizations issued the warnings**	**Warning content**
March 26	The 2025 Annual Threat Assessment issued by the US intelligence community.	China remains the top military and cyber threat to the US.
May 27	NATO and the European Union issued statements publicly expressing their support for the Czech Republic in response to cyberattacks.	It is assessed that Czech's CI was attacked by China's hacker group APT31.
August 27	A joint cybersecurity advisory was issued by 23 intelligence and security Services from 13 countries, including the US, UK, Canada, Australia, New Zealand, Germany, Italy, Japan, the Netherlands, Poland, Finland, the Czech Republic, and Spain.	The advisory points out that China's state-sponsored hacker groups have compromised critical infrastructure and networks worldwide.

Table 2: International warnings issued in 2025 regarding China's threats of cyberattacks

China has fully integrated its public and private resources across its military, intelligence, industry, and technology sectors. Through diverse hacking measures and technologies, China has enhanced penetration and concealment capabilities of its external cyberattacks. In response to these threats, the NSB will work with the national intelligence community and relevant government agencies, so as to report and address China's hacking operations targeting Taiwan in a timely manner through the established joint defense and reporting mechanisms on information security.

The NSB established cybersecurity cooperation with over 30 countries worldwide in 2025. Through information security dialogues and technical conferences, the NSB strives to obtain timely intelligence on attack patterns of China's cyber army. Furthermore, through networks of international information security cooperation, the NSB conducts joint investigations into malicious relay nodes, thereby supporting government decision making, response preparedness, and further enhancing the overall resilience and capacity of Taiwan's CI protection.

The NSB urges all nationals to raise their cybersecurity awareness and remain vigilant against cyber threats posed by China, so that we could jointly safeguard the comprehensive cybersecurity of Taiwan.