Analysis on China's Cyberattack Techniques in 2024

The PRC cyber force has repeatedly cracked into the cyber space belonging to the Republic of China (Taiwan) to steal data and conduct intrusions. Moreover, its techniques have become increasingly sophisticated and covered a wide range of targets, such as government agencies, critical infrastructure (CI) and high-tech manufacturing industry. Such efforts attempt to disrupt Taiwan's government operations, as well as gain advantages in the fields of politics, military, technology, and economy.

I. Trends and developments

1. Comprehensive status of China's cyber threats against Taiwan: According to the Indicators of Compromise from Taiwan's Government Service Network (GSN), the GSN received a daily average of 2.4 million cyberattacks in 2024, doubling the daily average of 1.2 million attacks in 2023 (as shown in Figure 1). In addition, most of the attacks are attributed to the PRC cyber force. Although many of them have been effectively detected and blocked, the growing numbers of attacks pinpoint the increasingly severe nature of China's hacking activities against Taiwan.

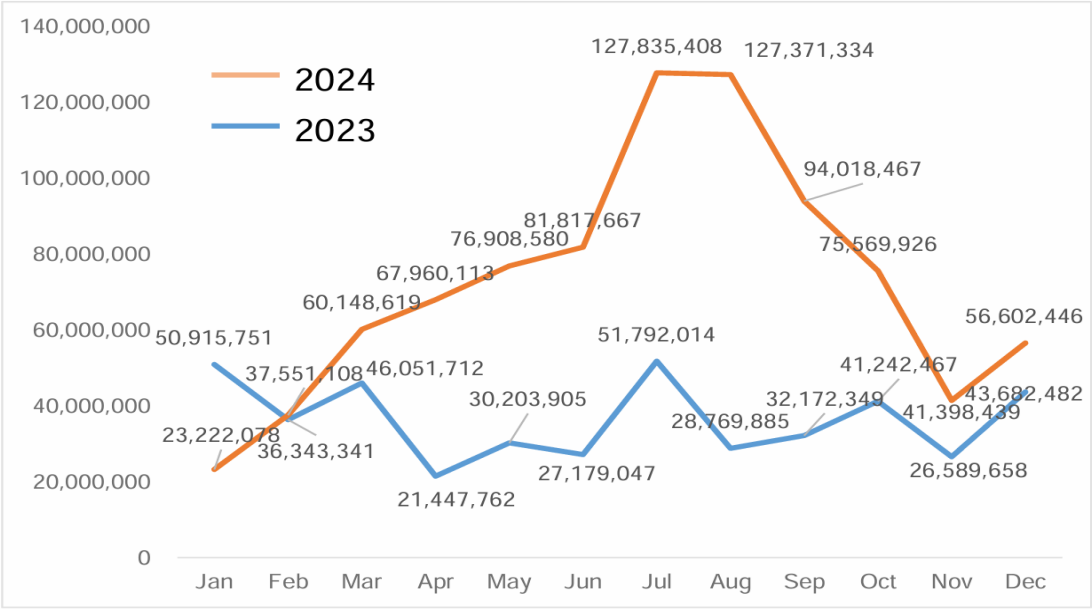

Figure 1: Comparison of cyber threat statistics between 2023 and 2024

2. Cyberattack cases related to PRC cyber force: In 2024, national intelligence community of the ROC reported a total of 906 cases of cyberattacks against Taiwan's government agencies and private sector. The number shows an increase of more than 20% when compared with 752 cases in 2023. Among all those cases of cyberattacks, attacking government agency accounts for the highest proportion, namely above 80%. In addition, after analyzing the targets of cyberattacks conducted by PRC cyber force, attacking communications field, mainly telecommunications industry, has grown by 650%, and attacking the fields of transportation and defense supply chain have grown by 70% and 57%, respectively. Attacks on these three fields have the most significant growth rates, showing that they are the key areas of China's chosen targets of cyberattacks (as shown in Figure 2).

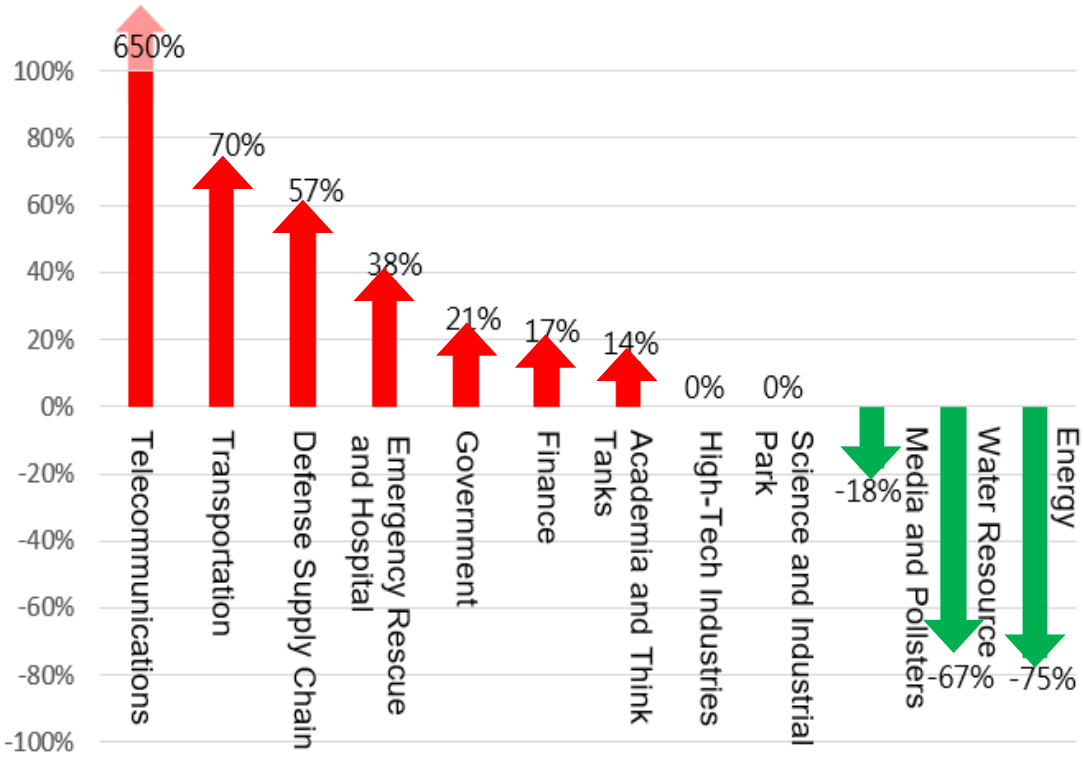

Figure 2: Statistics on the growth and decline rates of cyberattacks in different fields from 2023 to 2024

II. Cyberattack techniques

1. Targeting government agencies: The PRC cyber force targets vulnerabilities of Netcom devices used in Taiwanese government

agencies to set up ambushes and steal confidential information. On top of that, it makes use of techniques, such as Living off-the-land, to escape detection by network defense systems. A case in point is that PRC cyber force exploits vulnerabilities of email system to conduct cyberattacks against Taiwanese government agencies. Moreover, it targets Taiwanese civil servants' emails and launches cyberattacks, such as social engineering, attempting to steal confidential information.

2. Targeting information service providers (ISPs) and the defense supply chain: The PRC cyber force has employed diverse techniques to infiltrate and steal information from Taiwan's defense supply chain and ISPs. Particularly, the cyber force targets on suppliers providing services concerning email, official document, cryptographic, or personnel scheduling systems. Moreover, the scope of attacks is further expanded through the supply chain.

3. Infiltrating Taiwan's CI: In 2024, the PRC cyber force employed techniques consisting of advanced persistent threats, phishing mails, as well as the use of zero-day vulnerabilities, Trojans, and backdoors, attempting to infiltrate and compromise Taiwan's CI systems, such as those for highways and ports. In this way, China aims to disrupt Taiwan's order of transportation.

4. Conducting cybercrime through the techniques of military-civil fusion: With the support from private collaborative organizations, PRC cyber force conducts cyberattacks against Taiwan's manufacturers by utilizing ransomware or other cybercrime techniques in an attempt to obtain economic benefits. A case in point is that Taiwan's Criminal Investigation Bureau has recently identified that PRC cyber force carry out brute-force attacks against some Taiwanese academic institutes. A case in point is that Taiwan's Criminal Investigation Bureau has recently found China carrying out brute-force attacks against some Taiwanese academic institutes. Chinese hackers would modify system settings, such as adding dialing function to the local telephone systems. In this way,

Chinese scam syndicates could call out through those institutes to make scam calls.

5. Concealing the trace of cyberattacks and unveiling acquired information on the dark web: Chinese hackers steal personal data of Taiwanese nationals and sell those data on the dark web and hacker forums. Such moves aim to reap profits through the techniques of Hack & Leak. Moreover, they voice criticism of Taiwan's inability in cybersecurity on social media forums to undermine the prestige and credibility of the Taiwanese government.

6. Combining military exercises and cyberattacks: The PRC cyber force would launch cyberattacks on Taiwan's CI when the PLA conducts military drills against Taiwan. For example, it takes advantage of edge devices to carry out DDoS attacks on Taiwan's transportation and financial institutions, intending to intensify the harassment effect and military intimidation.

7. Targeting emerging industries to steal technologies: China also targets high-tech startups worldwide to steal patented technologies and gain its competitive advantage. In 2020, Cisco warned that Chinese hacker group APT41 exploited vulnerabilities in the products of prominent network equipment companies, such as Citrix and Cisco, in order to target enterprises globally, aiming to steal sensitive internal technique information.

8. Building a global stealth cyberattack network: China exploits Taiwan's vulnerabilities, such as passwords in Internet of Things (IoT) devices, to hack and control these devices. By encrypting and linking each of them, those devices together make up the stealth networks, aka Botnet, to carry out cyberattack activities.

III. Conclusion: China has continued to intensify its cyberattacks against Taiwan. By applying diverse hacking techniques, China has conducted reconnaissance, set cyber ambushes, and stolen data

through hacking operations targeting Taiwan's government, CI and key private enterprises. Making use of a joint ICT security defense mechanism, the Taiwanese government has ensured that the early-warning threat intelligence is gathered by a wide range of intelligence sources, as well as shared and responded in real-time with the competent authorities. The NSB urges all nationals to prioritize cybersecurity and remain vigilant against cyber threats posed by China, so that we could jointly safeguard the comprehensive cybersecurity of Taiwan.