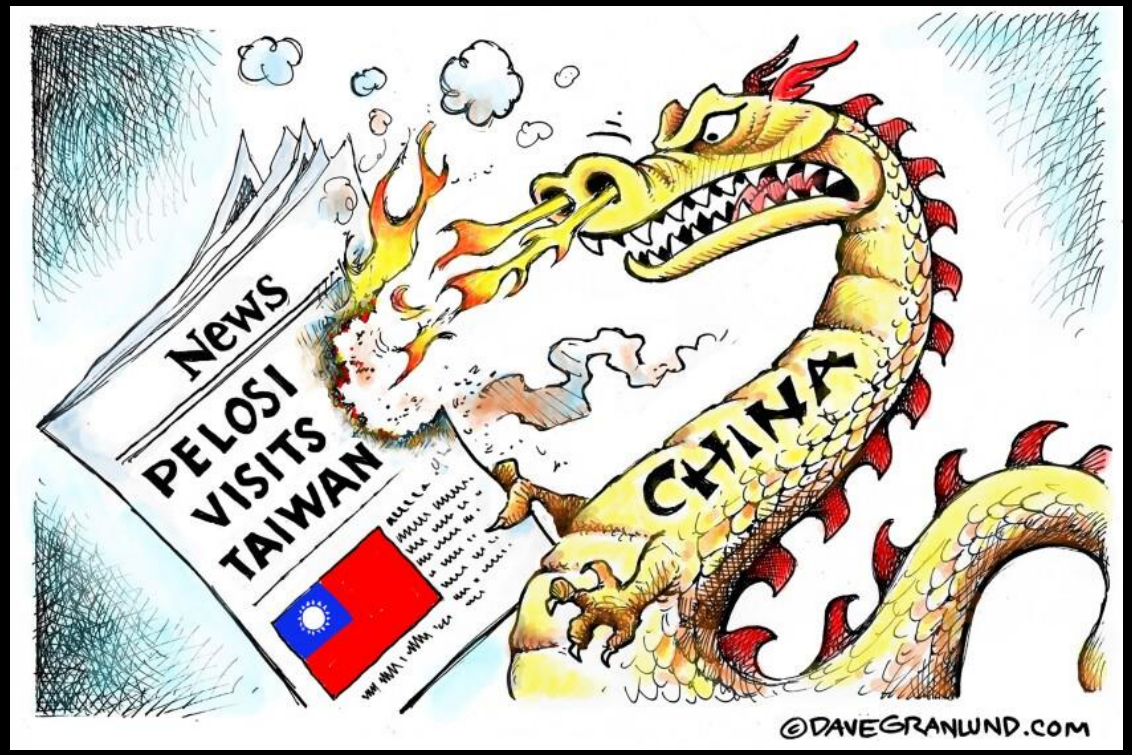
China‘s Offensive Cyber Ecosystem and Operations Against Taiwan

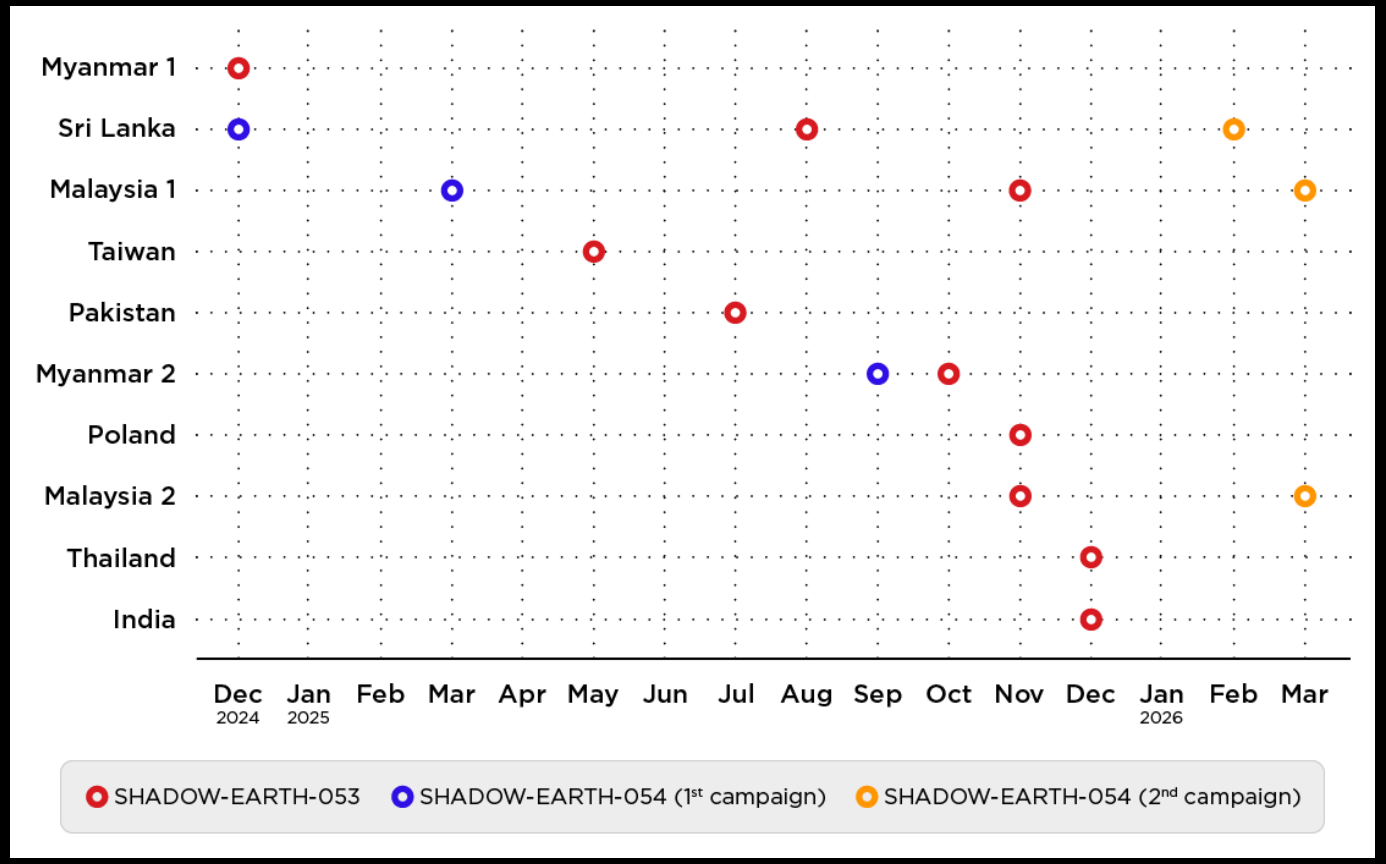
Chinese cyber and information campaigns against Taiwan

- Chinese cyberattacks persistently target Taiwanese telecommunications, academic institutions, government institutions, research organizations, and non-governmental organizations.
- Chinese disinformation target public opinion, creates new or exacerbates existing divisions, and undermines public trust in public institutions and democratic processes.
- While cyberattacks differ from disinformation operations in their methods and tools, both are considered part of information warfare (information warfare tactics)



Notable campaigns targeting Taiwan in 2025-2026

- March 2025 – Chinese group UAT-5918 targets critical infrastructure entities in Taiwan (Cisco Talos)
- July 2025 – Several Chinese threat actors run espionage campaigns against Taiwanese semiconductor manufacturing (Proofpoint)
- December 2025 - Leaked documents from the Chinese firm Zhongke Tianji reveal the use of generative AI to influence public opinion around Taiwan's elections (GMF)
- April 2026 – New Chinese threat actors targets government institutions in Taiwan and Southeast Asia (Trend Micro)



Source: Trend Micro

China’s Hacking Ecosystem

The State

People's Liberation Army (PLA)

- Historically active in industrial espionage and IP theft => military's use to support Chinese SOEs
- Since 2015, a more pronounced shift toward strategic in support of PLA intelligence needs => most "overseas" cyber missions are under MSS purview
- Strategic Support Force (2015–2024)

Ministry of State Security

- Collection of strategic intelligence, Industrial espionage
- Monitoring of dissidents (shared mission with the Ministry of Public Security)
- Front companies as identity cover for MSS offensive teams
- Contractors from private sector to fill gaps and offer flexibility
- Universities provide people (expertise) and infrasructure (e.g., Wuhan University, University of Electronic Science and Technology of China, Shanghai Jiao Tong University – ICST)

~~Strategic Support Force~~

Strategic Support Force

- Created as part of comprehensive reform of the PLA in 2015
- In 2024, disbanded into three separate parts
  - Information support force - likely focus on “informatization” and “information support” (i.e., securing communication) rather than offensive cyber operations.
  - Cyber force - likely where responsibility for wide range of offensive cyber lies (cyber intelligence, cyber espionage, offensive cyber, including sabotage, information preparation of battlefield)
  - Space force

A different type of threat actor: Volt Typhoon

- Target selection and behavioral patterns of the Volt Typhoon group (VANGUARD PANDA) do not correspond to traditional cyber espionage or intelligence operations.
- Subsequent findings indicate that Volt Typhoon was present in compromised systems for up to five years.
- To mask its activities, Volt Typhoon created a botnet (KV-botnet) composed of hijacked IoT devices.
- Volt Typhoon compromised the IT environments of several critical infrastructure organizations: primarily in the sectors of communications, energy, transportation systems, and water and wastewater systems.
- Volt Typhoon’s targeting is highly relevant for Taiwan
- Likely part of the PLA

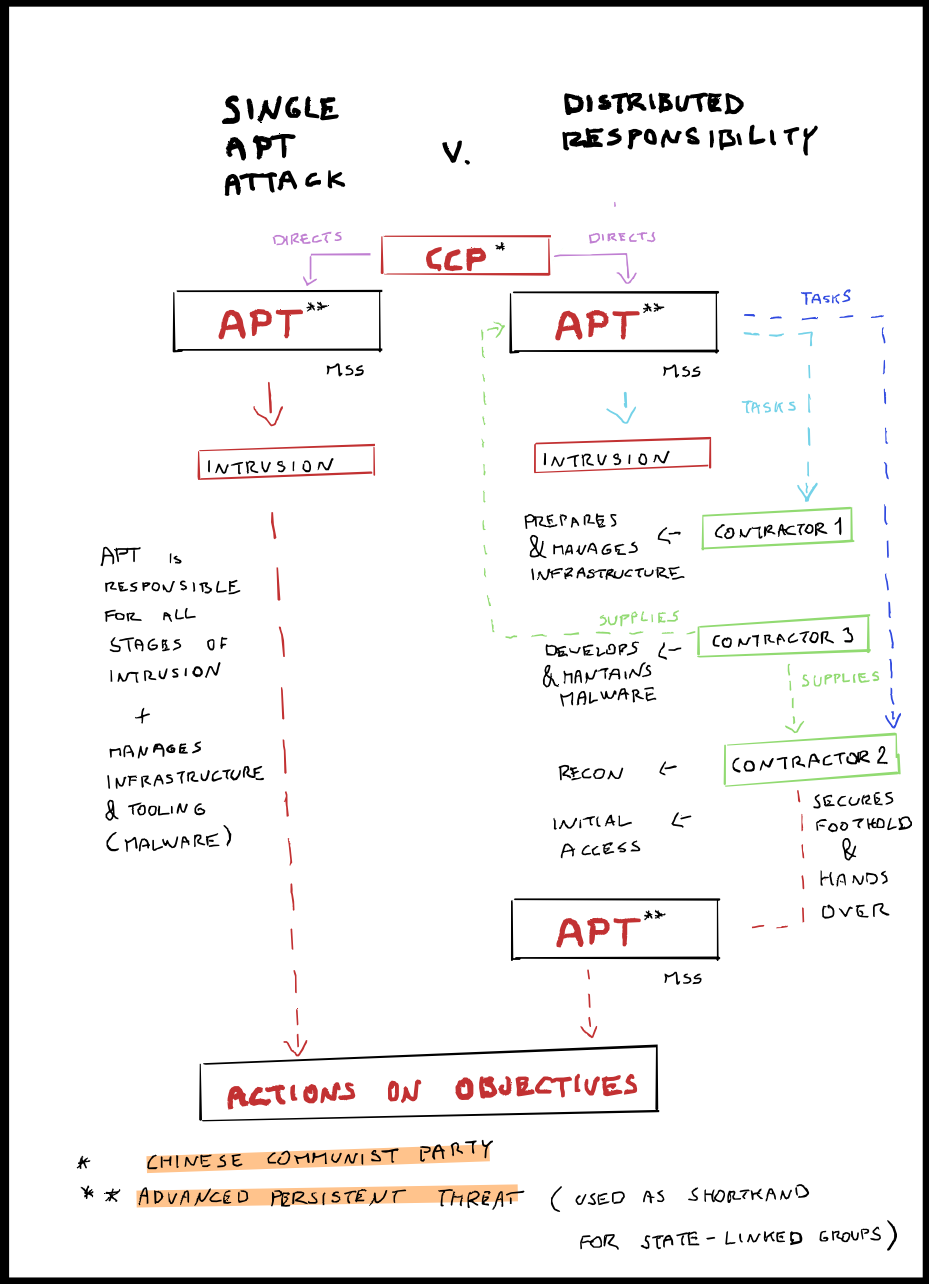
Private sector supports state operations

- **Compete for government contracts:** **PLA, MSS, MPS put out requests for offensive cyber operation and contractors bid for them**
- **Develop malware for state threat actors:** **some malware used by Chinese threat actors (TAs) was developed by contractors**
- **Take initial part in multi-actor intrusions:** **secure initial access, then hand over to government TA**
- **Prepare and manage infrastructure:** **IP ranges, domain registration, obfuscation networks -> Infrastructure-as-a-Service**

- **I-Soon (Anxun) aka Aquatic Panda:** A company founded by Wu Haibo, a former member of the "Green Army," i-Soon has been implicated in various state-sponsored hacking activities. Leaked documents revealed contracts with several public security bureaus and government entities, indicating their role in surveillance and hacking operations, including the targeting of dissidents and foreign organizations.
- **Chengdu 404 aka APT41:** This firm is another major player in the field of Chinese cyber contractors. It has participated in offensive cyber operations and is known for its ties to state security agencies.
- **Wuhan Xiaoruizhi S&T aka APT31:** Likely a front identity for the Ministry of State Security.
- **Hainan Xiandun Technology aka APT40:** Similar to Wuhan Xiaoruizhi, this firm likely functions as a front for government cyber operations.

New normal

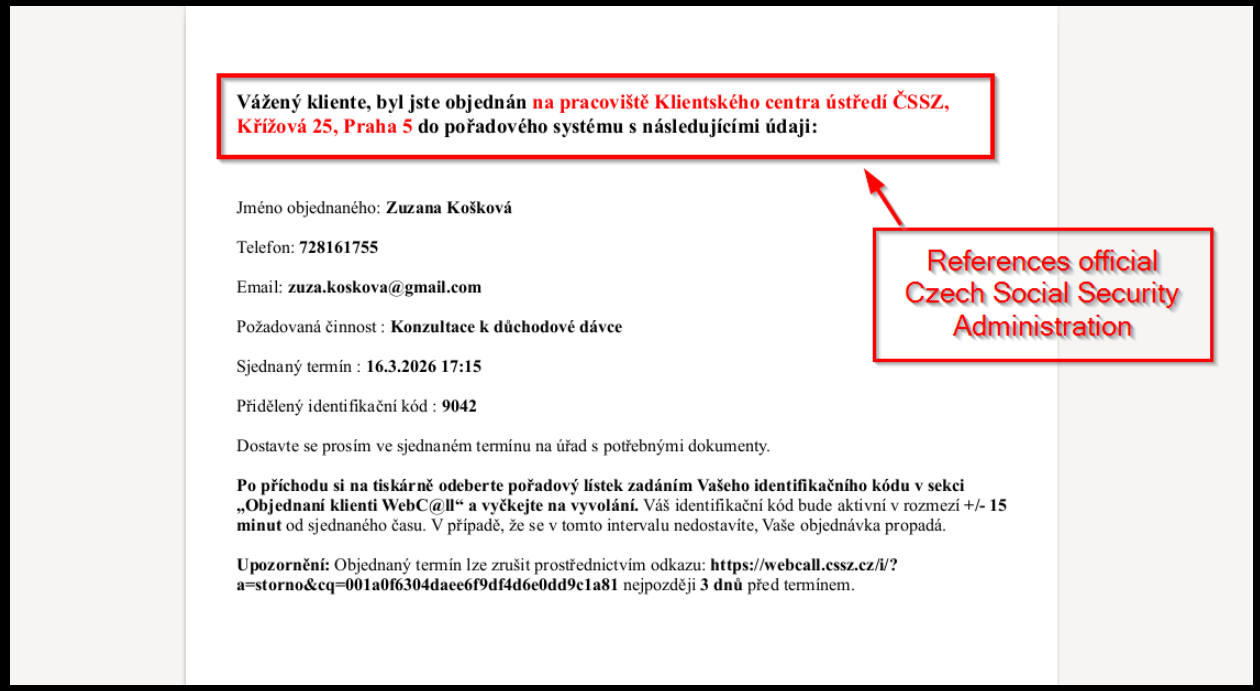
- Shift from single-actor attribution to a ”distributed responsibility" model: Chinese state-linked cyber activity has moved toward an ecosystem model in which responsibility for intrusions is distributed across military units, intelligence services, and private firms
- Tooling and infrastructure as separate accountability: privately developed tooling such as the ShadowPad backdoor has been sold across suspected PLA units and contractor networks, meaning vendors share responsibility alongside operators; separately, botnet infrastructure attributed to firms like Integrity Technology Group shows how companies can enable campaigns without directly executing intrusions.
- Salt Typhoon as the example: the 2025 attribution by the US and partners tied the campaign to multiple China-based entities including at least three private firms, contrasting with older cases like Mandiant's 2014 PLA Unit 61398 attribution and the 2017 APT3 indictment.



Case: Operation Dragon Weave

Operation Dragon Weave

- Made public by security company Sygnia in June 2026
- Analysis of malware sample revealed that uknown TA targeted government organizations and NGO both in Taiwan and Czechia in March 2026
- Taiwan: malicious document pretending to be a result of project review
- Czechia: fake CSSZ appointment targeting European Values researcher
- Czech targeting likely related to Senate President Vystrcil‘s visit to Taiwan in June 2026



Vážený kliente, byl jste objednán na pracoviště Klientského centra ústředí ČSSZ, Křížová 25, Praha 5 do pořadového systému s následujícími údaji:

Jméno objednaného: **Zuzana Košková**

Telefon: **728161755**

Email: **zuza.koskova@gmail.com**

Požadovaná činnost : **Konzultace k důchodové dávce**

Sjednaný termín : **16.3.2026 17:15**

Přidělený identifikační kód : **9042**

Dostavte se prosím ve sjednaném termínu na úřad s potřebnými dokumenty.

Po příchodu si na tiskárně odeberte pořadový lístek zadáním Vašeho identifikačního kódu v sekci „Objednaní klienti WebC@ll“ a vyčkejte na vyvolání. Váš identifikační kód bude aktivní v rozmezí +/- **15 minut** od sjednaného času. V případě, že se v tomto intervalu nedostavíte, Vaše objednávka propadá.

Upozornění: Objednaný termín lze zrušit prostřednictvím odkazu: **https://webcall.cssz.cz/i/?a=storno&cq=001a0f6304daee6f9df4d6e0dd9c1a81** nejpozději **3 dnů** před termínem.

References official Czech Social Security Administration

Source: [Operation Dragon Weave : Uncovering a China-Linked Campaign Targeting Czech Republic and Taiwan Using Azure Cloud C2]

CYBULE

www.cybule.cz
kontakt@cybule.cz