Recorded Future®

EXECUTIVE INSIGHTS REPORT | DEC 2025

China's Zero-Day Pipeline: From Discovery to Deployment

From Insikt Group®

Summary

China's observed use of zero-days has declined since 2023. However, it has expanded its capacity to discover and manage vulnerabilities, **signaling a continued effort toward stockpiling exploits** for strategic or military advantage.

The Data Security Law (DSL) and Provisions on the Management of Network Product Security Vulnerabilities (RMSV) **give the Chinese state first access and control over zero-days.** Combined with government-backed competitions, incentives, and private contractors, this framework likely sustains one of the world's largest reserves of exploitable vulnerabilities.

The creation of the Information Support Force (ISF) and Cyberspace Force (CSF) signals China's **consolidation of cyber capabilities**, likely enabling more effective offensive and defensive cyber operations, with vulnerabilities likely serving as a central resource.

Defenders should adopt an "assume breach" posture and build for containment, implementing **zero trust and layered defenses** to limit attacker movement and impact after an exploit.

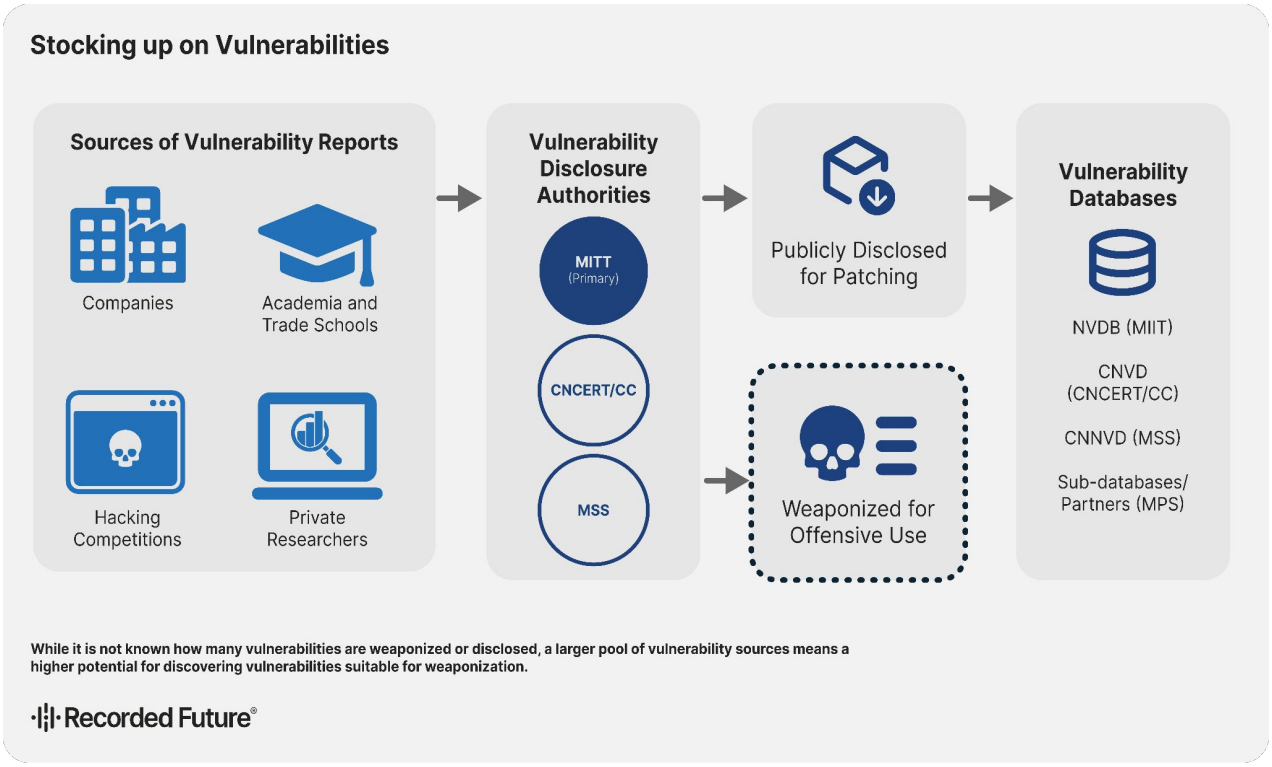


Figure 1: *How China stockpiles vulnerabilities (Source: Recorded Future)*

Zero-Days as Strategic Weapons

A zero-day is a previously unknown software flaw for which no patch exists at the time it is discovered or exploited. Once weaponized, it allows adversaries to gain access, escalate privileges, or execute remote commands. These capabilities are especially effective against perimeter and enterprise systems, where a successful compromise can provide initial access and allow attackers to maintain persistence and carry out further cyber actions.

Choosing whether to disclose or keep a zero-day vulnerability is a strategic decision. Governments must balance public safety with the potential intelligence or military value of keeping the flaw secret. In the US, this process is guided by the Vulnerabilities Equities Process (VEP), which is designed to be transparent and generally favors disclosure to help maintain internet security.

China's Vulnerability Management Regime

China's vulnerability management system is centralized and led by the state. Its laws, incentives, and institutions work together to feed new exploits and technical capabilities directly to the government, turning software vulnerabilities into strategic assets under state control.

- **Mandatory Reporting**

  The RMSV (2021) requires that all discovered vulnerabilities be reported to the Ministry of Industry and Information Technology (MIIT) within two days and prohibits disclosure to foreign entities. The Data Security Law (DSL) and National Intelligence Law (NIL) further compel all individuals and organizations to support state security objectives, with strict penalties for non-compliance. Together, these laws grant Beijing first access and complete control over all newly discovered flaws.

- **Incentivizing Compliance**

  This legal framework is reinforced through financial and professional incentives. The China National Vulnerability Database of Information Security (CNNVD), managed by the Ministry of State Security (MSS), offers researchers and firms monetary rewards, certificates, honorary titles, and preferential access to government contracts. This system encourages compliance by making vulnerability disclosure both mandatory and materially rewarding.

- **Talent Development and Recruitment Pipelines**

  China combines strict regulations with a well-organized system for developing cybersecurity talent. Competitions such as the Tianfu Cup, Matrix Cup, and QiangWang Cup serve as key recruitment and training platforms for the state's cyber programs. The 2024 Matrix Cup's $2.75 million USD prize pool, nearly twice that of Canada's Pwn2Own, highlights the size of this investment.

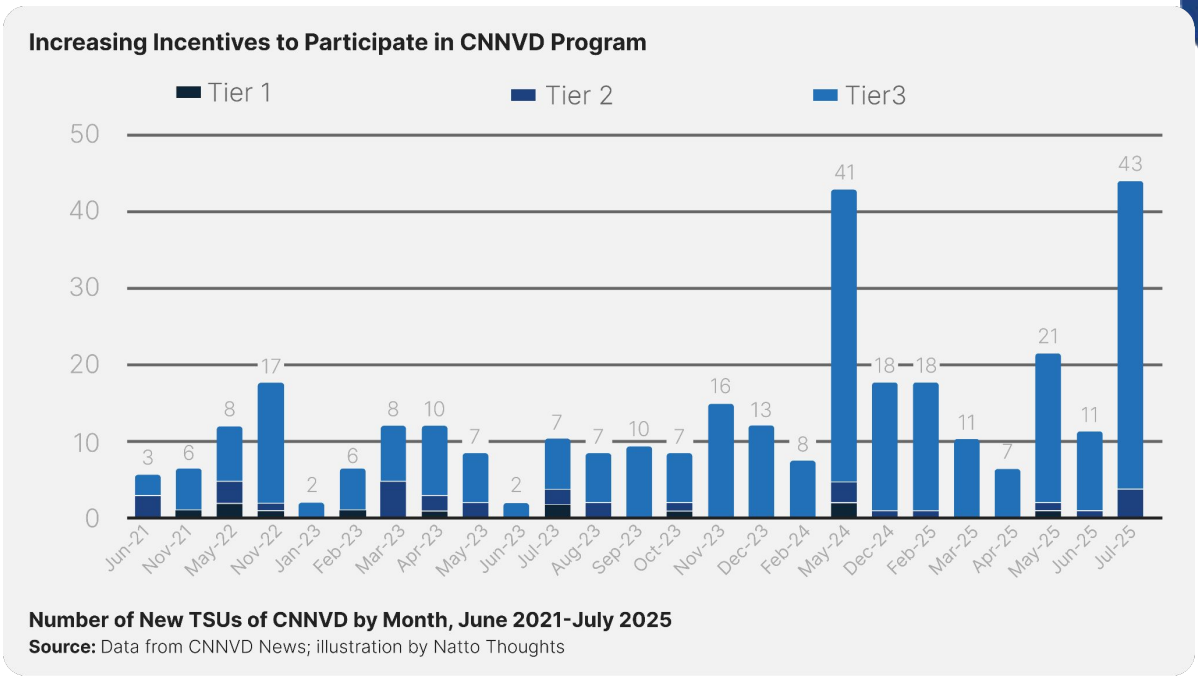
- **Private Sector Relationships**

  China's private sector also plays a pivotal role. Major firms such as Qi An Xin, Huawei, Qihoo 360, and NSFocus contribute vulnerabilities and technical expertise directly to the government. Large technology companies also fund or subcontract offensive work to smaller firms, creating a dense ecosystem of start-ups engaged in exploit research and hacking services. The i-SOON leaks (2023) revealed the scale and interconnectedness of this ecosystem: The company sold hack-for-hire services and targeting platforms to government customers while subcontracting work for Qi An Xin and Chengdu 404.

From Discovery to Deployment: Operationalizing China's Vulnerability Pipeline

This centralized vulnerability ecosystem is producing measurable results, enabling Chinese state-sponsored groups to convert vulnerability discovery into operational access at a speed and scale far beyond that seen in other national programs. A clear manifestation of this is their sustained focus on enterprise and edge technologies, including Fortinet, VMware/ESXi, and Ivanti, where access is durable and often high-privileged, and detection is limited. In 2025, China-linked groups exploited Ivanti VPN and Trimble Cityworks (1, 2) flaws as part of a long-term strategy to remain undetected within networks, expand access, and position themselves for potential critical infrastructure disruption.

China continues to expand its network of CNNVD technical support units (TSUs) and related programs, increasing its overall research base. TSUs are specialized organizations, often universities, state-linked labs, and cybersecurity firms that directly feed vulnerability research and intelligence into the national system. Since 2021, the number of TSUs has increased significantly, broadening the state's research capacity and deepening its ability to identify and operationalize software flaws at scale.



Number of New TSUs of CNNVD by Month, June 2021-July 2025
Source: Data from CNNVD News; illustration by Natto Thoughts

Figure 2: *Number of new CNNVD TSUs by month, June 2021 to July 2025 (Source: Natto Thoughts)*

Most vulnerability disclosures to affected vendors and the broader security community still originate from universities, labs, and cybersecurity firms associated with CNNVD, CNVD, and the expanding TSU network. However, even as the ecosystem grows, the overall volume of these disclosures continues to decline, indicating that a larger share of discoveries is now being routed internally rather than published. This suggests that more vulnerabilities are being withheld for state-directed use. Secrecy surrounding hacking competitions is also growing: The Tianfu Cup was not held publicly in 2024, and the 2024 Matrix Cup shared little to no details about discovered exploits. These competitions have historically been major sources of high-quality vulnerabilities, and reduced transparency further aligns with the shift away from open disclosure.

Together, these trends — the rapid expansion of TSUs, the decline in public vulnerability reporting, and the tightening secrecy around exploit-generation events — likely point to a deliberate state strategy that emphasizes centralized stockpiling and selective operational use of vulnerabilities rather than public disclosure.

Strategic Stockpiling and Selective Use

China's reported use of zero-days declined from twelve in 2023 to five in 2024, and it is responsible for only ten of the 104 zero-day exploits identified globally so far in 2025. While this may partly reflect limited visibility into zero-day deployment and attribution, the trend may also suggest a more selective, strategic approach to when and how its zero-day capabilities are used.

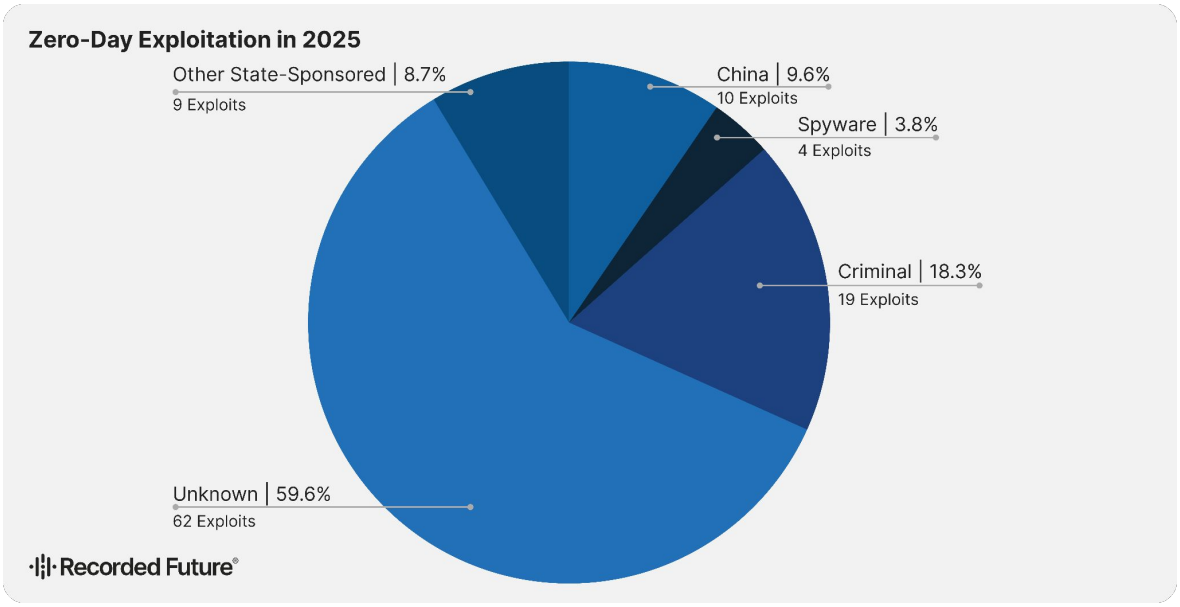


Figure 3: *Of the 104 zero-days identified in 2025, ten were attributed to Chinese state-sponsored threat actors (Source: Recorded Future)*

Beijing's control mechanisms under the RMSV and DSL enable it to selectively weaponize or withhold zero-days, preserving its most impactful capabilities for crises or strategic objectives. At the same time, n-day vulnerabilities — older but still unpatched flaws — remain highly effective due to inconsistent global patching.

Using these known flaws allows Chinese operators to gain access to networks and gather intelligence without revealing their zero-day exploits. Overall, this reflects a system designed for long-term preparedness rather than immediate gain.

Military Integration and Strategic Significance

China's April 2024 military reforms introduced three new divisions within the People's Liberation Army (PLA), including two centered on cyber and information security:

- The Information Support Force (ISF), which is responsible for the security and continuity of China's military networks, data systems, and command infrastructure
- The Cyberspace Force (CSF), which is dedicated to both offensive and defensive cyber operations

Together, the two units consolidate China's cyber and information capabilities, which were previously primarily nested under the PLA Strategic Support Force. These units form the backbone of its digital warfighting structure. The restructuring is likely to enhance Beijing's ability to coordinate kinetic and cyber operations, with zero-days serving as key enablers and potential first-strike tools.

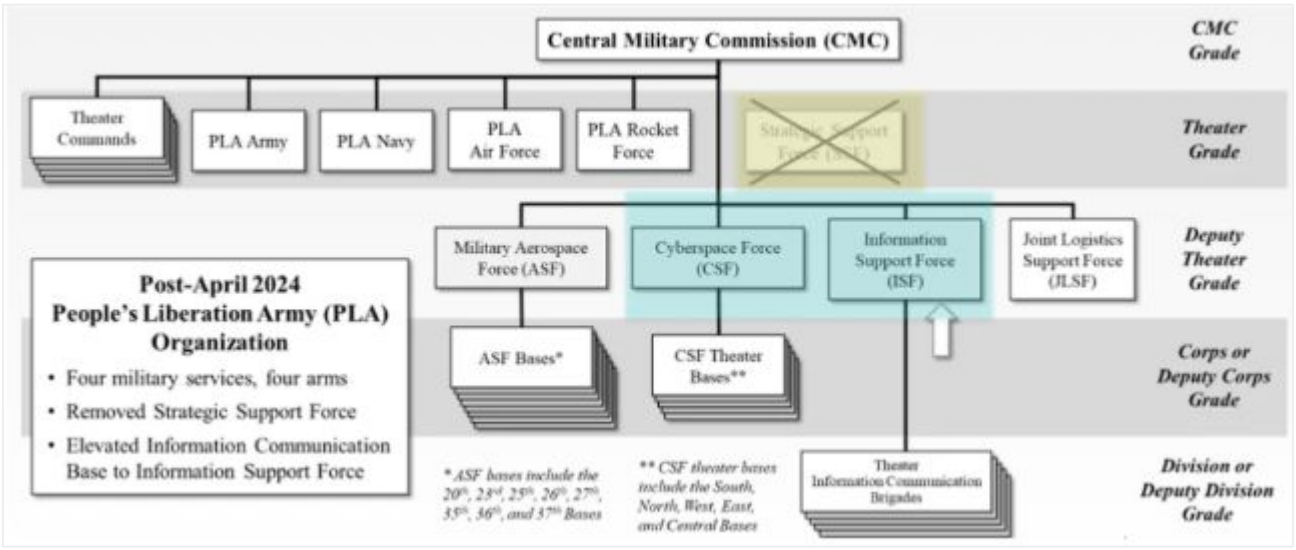


Figure 4: *New structure of the People's Liberation Army (PLA) (Source: The Jamestown Foundation)*

The future use of zero-days will depend on how China decides to pursue its geostrategic goals, such as future unification with Taiwan. However, by compromising critical networks in advance, China can secure persistent access and deploy disruptive cyber effects alongside kinetic operations, as seen in Russia's coordinated cyber-military campaigns in Ukraine. Chinese state-sponsored Volt Typhoon activity has been widely assessed as fulfilling such a purpose.

Outlook

Increased Willingness to Use Zero-Days: As China reduces its reliance on US technology through its "Delete America" campaign, the cost of exploiting Western software will decrease, making zero-day use more attractive in future conflicts over the long term.

Expanded Pre-Positioning: Expect continued infiltration of critical infrastructure and enterprise systems through both n-day and zero-day exploits to ensure durable wartime access.

Increased N-day Use: The rapid adoption of AI-assisted coding and automation is accelerating the accumulation of software vulnerabilities. This expanding security debt — the accumulation of unpatched and unreviewed vulnerabilities — will give adversaries, including China, a broader and more persistent pool of n-day exploits to weaponize.

Evolving Contractor Ecosystem: State-aligned private firms are likely to accelerate automation and AI-assisted vulnerability discovery, thereby expanding the Chinese state's operational stockpile of viable exploits.

Mitigations

Adopt an "Assume Breach" Posture: Implement zero-trust architectures that enforce identity and device verification at every access point. Use Recorded Future® Threat Intelligence to monitor for China-nexus infrastructure and malicious activity, feeding enriched indicators directly into security information and event management (SIEM) and security orchestration, automation, and response (SOAR) workflows.

Prioritize Edge and Enterprise Patching: Focus remediation efforts on virtual private networks (VPNs), firewalls, hypervisors, and identity platforms most commonly targeted by China-nexus threat actors. Use Recorded Future Vulnerability Intelligence to track emerging zero-day and n-day threats, prioritize patching by exploitation risk, and validate remediation across critical systems.

Detect Post-Exploitation Behavior: Use D3FEND mappings such as Process Access Pattern Analysis (D3-PAPA) and Remote Access Detection (D3-RAD) to identify stealthy follow-on actions. Combine these controls with Recorded Future Attack Surface Intelligence to identify exposed assets and verify that detection coverage extends to externally facing environments.

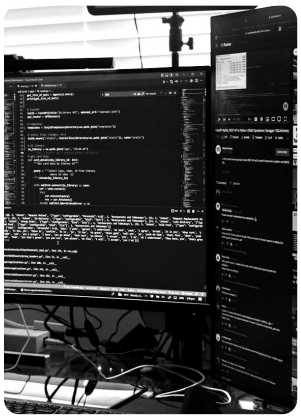
Secure Identities and Access: Leverage Recorded Future Identity Intelligence to detect compromised credentials that may complement exploit-based intrusions.

Further Reading

SOURCE	TITLE
Insikt Group	China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions
Insikt Group	Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group
Insikt Group	From Coercion to Invasion: The Theory and Execution of China's Cyber Activity in Cross-Strait Relations
Insikt Group	China's Ministry of State Security Likely Influences National Network Vulnerability Publications
IISS	China's new Information Support Force

Risk Scenario

Scenario: *EnerTech Global*, a European energy technology firm providing control systems and smart grid software to multiple NATO-aligned countries, becomes the target of a Chinese state-sponsored cyber campaign. Using undisclosed zero-day vulnerabilities, Chinese operators infiltrate EnerTech's production and customer environments to gather intelligence, manipulate software updates, and preposition for potential disruption.



First-order Implications

Threat

Chinese threat actors exploit a zero-day in a network management or VPN appliance to gain initial access to EnerTech's internal systems and engineering networks.

A zero-day in industrial control or software build pipelines is used to insert malicious code into firmware updates distributed to downstream customers.

Risk

Operational: Compromise of development and production networks halts manufacturing and disrupts customer support operations.
Legal: Breach of export-control and cybersecurity regulations triggers EU and US compliance investigations.
Brand: Public confirmation of a "state-backed breach" undermines trust with government and defense customers dependent on EnerTech's technology.

Second-order Implications

Threat

Attackers use stolen code-signing certificates to distribute trojanized software updates to energy utilities across Europe.

Collected intelligence on grid infrastructure is used to map potential disruption points for future contingency operations.

Risk

Operational: Some utilities see irregularities in their OT environments, including unexpected behavior in grid-monitoring tools, delayed telemetry updates, and unexplained authentication failures on systems that rely on EnerTech software.
Brand: EnerTech's reputation deteriorates as customers and regulators question its software assurance and supply chain controls.
Legal: Disclosure of tampered software triggers international incident response coordination and potential export-license suspension.

Third-order Implications

Threat

Persistent access enables China to remotely sabotage or disable systems during a geopolitical crisis, thereby amplifying disruption across allied power grids.

Stolen intellectual property is used by Chinese competitors to replicate EnerTech's industrial software, undercutting global market bids.

Risk

Competitive: Loss of proprietary code and technology enables China-based competitors to dominate regional procurement markets.
Brand: Association with a high-profile critical infrastructure breach erodes long-term credibility in both commercial and government sectors.
Legal: Multinational investigations and sanctions create enduring compliance exposure and financial penalties.

Key
Legal or compliance failure: Breach of laws, regulations, or industry standards resulting in liability or sanctions.
Operational disruption: Interruption to normal business processes affecting productivity or service delivery.
Brand impairment: Damage to reputation that reduces customer trust and market value.
Financial fraud: Unauthorized manipulation or theft of financial assets for personal or organizational gain.
Competitive disadvantage: Loss of market position due to inferior capabilities, intelligence, or innovation.

References:
The Risk Business: Second Edition
Intelligence to Risk
The Intelligence Handbook