STUDY

Not Out Of Control

Why China Tolerates Irresponsible Behavior In Its Cyber Campaigns – And How To Respond

Dr. Sven Herpig

November 19, 2026

Tech analysis and policy ideas for Europe

interface

Executive Summary

The PRC's cyber campaigns are widely read as an ecosystem that the government in Beijing no longer fully directs. A senior FBI official has said publicly that the Chinese "hacker-for-hire ecosystem has gotten out of control", and indictments have called it reckless and indiscriminate. The evidence supports a different reading. **The central government has not lost control of its cyber campaigns. It tolerates the looseness they produce, as the price of operating at scale.** This matters for affected states: a government that tolerates looseness is likely to change course only when keeping it costs more than dropping it.

A system built for scale. Over more than a decade, the PRC put in place the laws, institutions, force structure, and talent base needed to run many cyber campaigns in parallel. It also drew in a commercial market in access, infrastructure, and tooling that grew largely on its own. Reporting duties send newly found vulnerabilities to the state, which stockpiles them for selective use and also buys exploits for operations at scale. Beijing controls the security bureaus, but tasking is spread across the provinces and part of the work is contracted out. AI is being built into the intrusion chain. Dutch military intelligence assesses that the PRC's offensive cyber capabilities are now probably on par with those of the United States.

Control is bounded, not lost. The central government lets its operators work loosely, within a lower limit it enforces and an upper limit that has so far held. Between the two, contractors compromise targets on their own initiative and sell the results to state buyers, espionage blends with financially motivated crime, and tools and exploits spread after use. The central government corrects none of this. Since 2021, more than twenty enforcement actions have suspended leading firms from military procurement or excluded them from it. They all concerned how the firms won contracts. None concerned how they operate. Enforcement against cyber-enabled fraud shows that the state can correct at scale, and the criminal and contractual instruments that could reach operators have recently been strengthened. Correction reached how operators operate only once: around the 2015 US–China agreement, after sustained pressure on the relationship as a whole. The effect did not last. **A state that can correct and does not has made a choice.**

The upper limit – the ceiling – has not been tested. No PRC campaign has been shown to aim at disrupting the operation of foreign critical infrastructure, although access to power, water, and transport systems has been held for years. Restraint is likely part of the explanation, but some of that access may not be

enough for disruption, and no situation has yet arisen in which disruption would have served a Chinese objective. Access that PRC actors hold in critical infrastructure should be treated as access they may one day use to disrupt it.

Responsibility does not depend on tasking. A state that builds up the system, declines to correct how it runs and keeps buying what it produces is responsible for that output, whether or not it ordered each intrusion. Whether the state ordered a specific intrusion only shows how the campaign was run. It does not limit the state's responsibility.

More campaigns ahead. The number of PRC cyber campaigns is likely to rise, as AI and a competitive supplier market make operations cheaper. Operators are likely to care less about being named, even as they invest in staying undetected, and the gap between disciplined elite operations and loose contractor work is likely to widen.

The gap lies in the costs. Affected states have attributed, indicted, sanctioned, and taken down infrastructure, and the PRC has absorbed it. The activity stays below the threshold at which a decisive political response becomes likely. Responses mostly address single incidents and not the pattern they form, and rely mainly on technical instruments. The economic and diplomatic channels to which the PRC has visibly reacted in the past remain largely unused for cyber conduct.

Seven measures for affected states. None requires new legal powers. Two things are still missing, though: a shared record and a response agreed in advance.

- **Default attribution** comes first, and the others support it: hold the PRC responsible by default for its share of any campaign with a China nexus, without first proving that it tasked the specific intrusion.
- **Supply-layer disruption** takes down infrastructure that many operators share and produces evidence under judicial authority.
- **Personal attribution** names the firms, universities, individuals, and bureaus behind an intrusion set.
- **Collective cost imposition** uses the accumulated record for economic and diplomatic measures. Willing states act together and agree beforehand to share the cost of Chinese counter-pressure.
- **Ceiling contingency** prepares for the disruption of critical infrastructure: continuity planning for an adversary already inside, a coalition response agreed in advance, and a public statement that even holding such access will draw consequences.

- **Record consolidation** turns the evidence affected states already hold into one continuous, shared record.
- **Resilience** reduces what intrusions yield, pays off whatever Beijing decides, and can be started by a single state today.

What would change this assessment. The central government correcting how its operators behave in the field; a PRC campaign aimed at disrupting the operation of critical infrastructure; or a measurable change in PRC behavior after a group of affected states imposes costs together.

The PRC built up the system, tolerates how it runs, and keeps buying what it produces. The delegation is the policy, and affected states are entitled to respond to it as such.

Table of Contents

Executive Summary 2

1. Introduction: PRC's Campaigns Out Of Control? 7

2. System: Built For Scale 13

- 2.1 Regulatory Framework 14
- 2.2 Policy Ecosystem 18
- 2.3 Force Structure 22
- 2.4 Talent Base 26
- 2.5 Tooling And Access 28
- 2.6 System Findings 30

3. Control: Bounded, Not Lost 32

- 3.1 Tolerated Looseness 34
- 3.2 Selective Correction 37
- 3.3 Operational Ceiling 42
- 3.4 Countervailing Evidence 44

4. Record: Campaigns Examined 47

- 4.1 AI Automation (GTG-1002) 47
- 4.2 Untested Tooling (React2Shell) 49
- 4.3 Shared Tooling (PlugX) 50
- 4.4 Exploit Proliferation (ProxyLogon) 52
- 4.5 Contractor Initiative (i-SOON) 54
- 4.6 Mission Blending (APT41) 55
- 4.7 Case Findings 56

5. Assessment: Normalized Statecraft 57

- 5.1 Delegation As Policy 57
- 5.2 State Responsibility 57
- 5.3 System Trajectory 60
- 5.4 Disincentive Gap 63

6. Response: Measures Available 69

6.1 Default Attribution 72

6.2 Supply-Layer Disruption 74

6.3 Personal Attribution 77

6.4 Collective Cost Imposition 79

6.5 Ceiling Contingency 82

6.6 Record Consolidation 84

6.7 Resilience 86

7. Conclusion: The Delegation Is The Policy 90

Appendices 92

I. Research 92

II. Acknowledgments 93

1. Introduction: PRC's Campaigns Out Of Control?

Over the past three years, more publicly reported state-backed cyber incidents outside the context of armed conflict have been traced to the People's Republic of China (PRC) than to any other state, followed by Russia.[1] There is a reason for this increase.[2] **The PRC has built up, sustains and draws on an ecosystem that runs a large number of cyber campaigns in parallel.**[3] It is among the states integrating Artificial Intelligence (AI) tools furthest into the intrusion chains of its cyber operations, based on the evidence available.[4] Many of its campaigns start broad and indiscriminate and become selective only afterward. Since at least the mass exploitation of Microsoft Exchange servers in 2021, PRC-linked operators have repeatedly compromised large numbers of exposed systems at once, and only

1 The European Repository of Cyber Incidents recorded 331 state or state-affiliated incidents between October 16, 2023 and October 15, 2026. Outside of armed conflict [manual selection for Russian war against the Ukraine], the PRC was the country of origin of 87 of those incidents, followed by Russia with 54. See European Repository of Cyber Incidents (2026): Detailed Table View. The relevant cyber campaigns are those the PRC conducts as an instrument of statecraft during strategic competition, below the threshold of armed conflict, rather than those conducted as part of an armed conflict. This paper focuses on state-enabled incidents that occur outside the context of armed conflict. It therefore excludes cyber operations integrated into active military hostilities, which are governed by international humanitarian law and follow a different escalation logic. It does not exclude military actors as such: espionage, intelligence preparation, and the pre-positioning of access in critical infrastructure are competition-phase activities that the PLA and its reserves conduct in peacetime, and that China's civil-military fusion deliberately blends with the work of the civilian security services and their contractors. Where PLA-related structures and policies build or run campaigns waged outside armed conflict, they are in scope; where a cyber capability would be employed only within a conflict, it is not. The dividing line is the strategic context, not the identity of the operator.

2 Other work explains the rise mainly through intensifying competition between major powers. That explanation addresses why demand for these operations has grown. The account offered here addresses how the PRC meets that demand, and why it tolerates the looseness that results. The two are compatible. See Kristan Stoddart (2025): China And Its Embrace of Offensive Cyberespionage & Thomas F. Lynch III (2024): Forward Persistence in Great Power Cyber Competition: Military Assets in a Relative Power Erosion Framework & Ryan Clarke, Dave Ormrod, Yihao Lim, and Jill Slay (2023): The Evolution of Chinese Cyber Offensive Operations and Association of Southeast Asian Nations (ASEAN)

3 E. g. Dakota Cary and Eugenio Benincasa (2024): Capture the (red) flag: An inside look into China's hacking contest ecosystem & Kieran Green (2025): Mobilizing Cyber Power: The Growing Role of Cyber Militias in China's Network Warfare Force Structure & Winnona DeSombre Bernsen (2025): Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace & Eugenio Benincasa (2024): From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem

4 E. g. Anthropic (2025): Disrupting the first reported AI-orchestrated cyber espionage campaign & NetAskari (2026): Robobox: Self driven malware creation and execution – made in China & Tim Starks (2026): Researchers observe first 'near-autonomous' AI attack on government target in Taiwan

then picked out those worth pursuing.[5] By these means, the PRC combines the capacity and the capability to sustain cyber campaigns against adversaries and partners alike. And these campaigns produce tangible returns: they yield political and military intelligence[6], advance the industrial and technological priorities of the PRC's successive Five-Year Plans[7], collect access to critical infrastructure[8] for a potential future conflict[9], and locate individuals abroad whom the state regards as political threats.[10] These campaigns are well documented. In Europe, for example, between 2022 and 2023, a single Chinese vendor's products were used to compromise more than 65,000 devices across six EU member states. A second firm provided offensive services directed at the critical infrastructure and critical functions of member states. Both were placed under EU sanctions in March 2026, together with two individuals named as co-founders of the second company.[11]

Set against these returns, the costs have so far been negligible for the PRC. Affected states have imposed consequences – official public political attributions, indictments, sanctions[12], and the court-authorized dismantling of operational

5 Council of the European Union (2021): China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory & ESET Research (2021): Exchange servers under siege from at least 10 APT groups & Microsoft Threat Intelligence (2025): Silk Typhoon targeting IT supply chain & CJ Moses (2025): China-nexus cyber threat groups rapidly exploit React2Shell vulnerability (CVE-2025-55182)

6 E. g. Bundesnachrichtendienst et al (2025): Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

7 Sveva Vittoria Scenarelli (2026): Understanding modern Chinese cyber operations means shifting from 'APT' to composite responsibility

8 This includes entities that enable mass downstream access, such as IT service providers. See for example: Aleksandar Milenkoski and Luigi Martire (2025): Operation Digital Eye | Chinese APT Compromises Critical Digital Infrastructure via Visual Studio Code Tunnels

9 E. g. Cybersecurity & Infrastructure Security Agency (2024): PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

10 Eugenio Benincasa (2026): How China's Cyber Operations – and the Contractors Behind Them – Target Critics Abroad

11 Council of the European Union (2026): COUNCIL DECISION (CFSP) 2026/588 of 16 March 2026 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States & Council of the European Union (2026): COUNCIL IMPLEMENTING REGULATION (EU) 2026/589 of 16 March 2026 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States & Council of the European Union (2026): COUNCIL REGULATION (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States & Council of the European Union (2026): Cyber-attacks against the EU and its member states: Council sanctions three entities and two individuals & National Cyber Security Centre (2026): China-linked malicious actors called out by UK and international partners for targeting sensitive data globally

12 E. g. Christina Rupp and Alexandra Paulus (2023): Official Public Political Attribution of Cyber Operations – State of Play and Policy Options

infrastructure[13] – mostly one incident at a time, and within the cyber domain. But the PRC has largely accepted these costs and carried on as before. The one exception came around the 2015 US–China agreement, when Chinese commercial cyber espionage against US firms fell for a few years after sustained US pressure that engaged the relationship as a whole.[14] Dutch military intelligence now assesses that the PRC "probably stands on an equal footing with the United States in the area of offensive cyber capabilities"[15], and **the PRC's geopolitical and economic weight makes uncoordinated responses by individual states both costly and ineffective. The PRC will therefore likely not only continue but expand its use of cyber campaigns as a normalized tool of statecraft.**

Affected states – among them the United States, the member states of the EU, Australia, and Japan – are left with few good options. One of them is to impose costs collectively: to raise, together, what these campaigns cost the PRC, with economic and diplomatic measures as well as those aimed at its cyber operations, such as takedowns of the underlying campaign infrastructure. In May 2025 the Czech Republic publicly attributed a campaign against its foreign ministry to an actor associated with the Chinese Ministry of State Security (MSS), and the EU and NATO issued statements of solidarity. No further consequence for the PRC followed.[16] **The Union's own statement recorded that malicious cyber activity linked to the PRC and directed at member states has increased in recent years, and that several member states have attributed comparable activity at national level since 2021.**[17]

13 E. g. U.S. Department of Justice (2024): Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers & U.S. Department of Justice (2026): Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure & TDR Team and Félix Aime and Charles Meslay (2024): Unplugging PlugX: Sinkholing the PlugX USB worm botnet

14 Adam Segal and Lorand Laskai (2018): A New Old Threat – Countering the Return of Chinese Industrial Cyber Espionage

15 Alexander Martin (2026): China's cyber capabilities now equal to the US, warns Dutch intelligence and see also: Office of the Director of National Intelligence (2026): Annual Threat Assessment of the U.S. Intelligence Community

16 National Cyber and Information Security Agency (2025): The Czech Government Has Publicly Attributed Cyberattacks to China: Actor APT31 Linked to the Chinese Ministry of State Security Has Targeted the Infrastructure of the Czech Ministry of Foreign Affairs & Ministry of Foreign Affairs of the Czech Republic (2025): Statement by the Government of the Czech Republic & North Atlantic Treaty Organization (2025): Statement of solidarity by the North Atlantic Council concerning the malicious cyber activities against the Czech Republic & Karel Janicek and The Associated Press (2025): The U.S., EU, and NATO are rallying behind the Czech Republic, which says a hacking group associated with China's government attacked its critical infrastructure

17 Council of the European Union (2025): Cyber: Statement by the High Representative on behalf of the European Union on malicious behaviour in cyberspace against Czechia

How cost imposition can change the PRC's behavior in the cyber domain depends on whether the central government is in control of its cyber operations. The looseness[18] in the PRC's cyber ecosystem – activity by the operators the state relies on that no one appears to have directed case by case – is real and readily documented: contractors compromise targets on their own initiative and sell the results afterward,[19] operators blend state espionage with private profit,[20] and exploits proliferate after a patch is released.[21] At this scale and over this many years, the question is whether such activity could continue without at least the acceptance of the central government. Either the PRC's cyber campaigns are out of control – organizationally and technically beyond the reach of the state that hosts them – or the central government could rein them in and has chosen not to.

Some officials take the first reading. A senior FBI official stated publicly in April 2026 that the Chinese "hacker-for-hire ecosystem has gotten out of control", describing a network of private companies and contractors that casts a wide net for vulnerable systems and sells what it finds to the government or, failing that, to others.[22] Indictments brought the previous year characterized the same ecosystem as reckless and indiscriminate.[23] On that reading, the PRC has failed to manage the looseness rather than chosen it. In both cases, affected states can press Beijing. The difference lies in what they press for. A government that had lost control could be pushed to get it back, and would have its own reasons to want that. A government that tolerates the looseness because it is the price of working at scale is being asked to give up a policy, and will not do that until keeping it costs more than dropping it.[24] **The evidence points to the second.**

18 "Looseness" is used descriptively, for the gap between what the state's operators do and what anyone can be shown to have directed. It does not presuppose whether that gap is lost or tolerated. The criterion of operational control comes from the companion framework, and the distinction between delegation and looser forms of state involvement from the literature on cyber proxies. See Sven Herpig (2025): Assessing Irresponsibility in Cyber Operations – A Guide for Operators and Decision-Makers in Times of Strategic Competition & Tim Maurer (2018): Cyber Mercenaries: The State, Hackers, and Power

19 Natto Thoughts (2026): i-SOON Leaks

20 Nalani Fraser, Fred Plan, Jacqueline O'Leary, Vincent Cannon, Raymond Leong, Dan Perez, and Chi-en Shen (2019): APT41: A Dual Espionage and Cyber Crime Operation

21 Orange Tsai (2021): A New Attack Surface on MS Exchange Part 1 - ProxyLogon!

22 AJ Vicens (2026): Chinese Hackers Vulnerable to US Arrest if They Travel, FBI Official Says & Jessica Lyons (2026): FBI cyber boss: China's hacker-for-hire ecosystem 'out of control'

23 U.S. Department of Justice (2025): Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns

24 Daniel W. Drezner (2011): Sanctions Sometimes Smart: Targeted Sanctions in Theory and Practice

Central control over the PRC's offensive cyber ecosystem has increased in recent years, through the consolidation of military cyber forces,[25] the tightening of a state-directed vulnerability pipeline,[26] and a demonstrated ability to adapt tooling and infrastructure at speed through contractor networks.[27] The government has also shown that it will discipline the companies it relies on: since 2021, more than twenty enforcement actions have suspended leading firms from military procurement or excluded them from it.[28] What is routinely disciplined, however, is how those firms win contracts, and not how they operate. The PRC's looseness is therefore better described as bounded delegation: the central government hands execution to others and accepts a certain level of looseness instead of correcting it.[29] The delegation has limits: contractors are disciplined when their conduct touches the state's own interests, and access held in foreign critical infrastructure has not been used in a campaign aimed at disrupting the systems themselves. **This shifts the question from whether the PRC is in control, yes or no, to something that can be observed: how much looseness the government tolerates before it steps in.**[30] For affected states, the policy question then becomes how to raise the cost of that tolerance until correcting its operators is cheaper for the PRC than keeping the looseness.

Whether a state exercises operational control over its cyber campaigns has become a benchmark for assessing irresponsible behavior in the cyber domain: control that is deliberately abandoned or unintentionally lost signals heightened risk.[31] The

---

25 Dave Aitel, Sophia d'Antoine, Winnona DeSombre, Isabella Garcia-Camargo, Ian Roos, Nicholas Rostow, Jonathan Smith, Alison Strongwater, Abraham Wagner, and JD Work (2022): China's Cyber Operations The Rising Threat to American Security & Kieran Green (2025): Mobilizing Cyber Power: The Growing Role of Cyber Militias in China's Network Warfare Force Structure & Devin Thorne (2025): China's Militia Forces Train to "Get Strong" in the New Era

26 Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities & Dakota Cary and Eugenio Benincasa (2024): Capture the (red) flag: An inside look into China's hacking contest ecosystem

27 Natto Thoughts (2026): i-SOON Leaks

28 Eugenio Benincasa and Natto Team (2026): China's Cybersecurity Powerhouses Face PLA Procurement Curbs

29 Bounded delegation is not a further point on the spectrum of state responsibility, which ranges from attacks a state prohibits to attacks it carries out itself. It describes how one state spreads its campaigns across much of that spectrum at once – from operations its own units execute, through contractor work it orders or shapes, to activity it ignores – and where it draws the lines it enforces. See Jason Healey (2012): Beyond Attribution: Seeking National Responsibility in Cyberspace.

30 The same pattern appears in the PRC's handling of its large technology companies. They were given wide latitude while they served the state's development goals and were brought under sharp control from 2020 onward – among other steps, the Ant Group listing was halted and Didi was placed under cybersecurity review – once the government judged them a risk to financial stability and to data and national security. See Ya-Wen Lei (2023): The Gilded Cage: Technology, Development, and State Capitalism in China.

31 Sven Herpig (2025): Assessing Irresponsibility in Cyber Operations – A Guide for Operators and Decision-Makers in Times of Strategic Competition

PRC fits neither description cleanly. **It has not lost control.** It has increasingly consolidated control over the system its campaigns run on – the military and civilian security services, their provincial and municipal bureaus, state-owned and private contractors, universities, and the militia reserve drawn from them – and drew in a commercial market in access, infrastructure, and tooling that grew largely on its own, shaping it through regulation and procurement.[32] It left the looseness that this system produces uncorrected and continued to buy the output, tolerating it as the price of scale. For affected states, the difference matters less than it seems. Tolerating looseness it could correct makes the PRC just as responsible as if it had lost control. **Where a state builds up a system, draws on it, and tolerates how it runs, the delegation is the policy.** The most important measure that follows is to treat the PRC as responsible by default wherever a campaign has a China nexus, and the other measures in Chapter 6 help apply that default.

The paper is organized as follows.

- **Chapter 2** sets out how the PRC built a system for running cyber campaigns at scale: reporting duties, institutional pipelines, force structure, a talent base, and the commercial market it draws on.
- **Chapter 3** establishes where the central government's control is tight and where it tolerates looseness, by examining what it corrects and what it declines to correct.
- **Chapter 4** tests that reading against six documented cases.
- **Chapter 5** assesses what this means: for the PRC's responsibility, for how its campaigns will develop, and for why the costs imposed so far have not worked.
- **Chapter 6** sets out seven measures available to affected states, aimed at the system that produces the operations, from disruption and attribution to collective cost imposition beyond the cyber domain.
- **Chapter 7** concludes. It names three developments that would change this assessment: the government correcting how its operators behave, a PRC campaign aimed at disrupting the operation of critical infrastructure, and a change in PRC behavior after affected states impose costs together.

32 The market did not develop in parallel with the state's own structures. Beijing encouraged the patriotic hackers of the late 1990s and 2000s to move into industry, the commercial market accelerated from the mid-2010s, and commercially provided obfuscation networks and botnets appeared at scale only from around 2021. See Scott J. Henderson (2007): The Dark Visitor: Inside the World of Chinese Hackers & Michael Raggi (2024): IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders & U.S. Department of Justice (2024): Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers

2. System: Built For Scale

The PRC's cyber campaigns run on a system built for scale. Over more than a decade, the PRC assembled the legal obligations, the institutional pipelines, the force structure, the talent base, and the access to tooling that a sustained, parallel campaign tempo requires. Most of that is documented in openly available sources or has been made available by researchers and practitioners, and through leaks.[33] Much of it can be observed: what the state put in place, whom it drew in, and what the system now produces. **Taken together, what the PRC has built and drawn in functions as an industrialized production system for cyber campaigns.** The term describes how the system works, judging by its output. It does not claim that Beijing planned it this way from the start, and parts of it, such as the commercial market, grew largely on their own. Industry analysis of the April 2026 international joint government advisory on Chinese threat actor operations reaches the same characterization.[34]

The five layers of that system are shown in Figure 1 and taken in turn below: the legal obligations that route vulnerabilities to the state (2.1), the policies that set its direction and turn those obligations into a supply chain (2.2), the force structure that runs operations (2.3), the talent base that staffs it (2.4), and the tooling and access it runs on (2.5), before 2.6 draws them together.

33 E. g. Atlantic Council (2026): Cyber Statecraft Initiative & Natto Thoughts (2026): Substack & Stanford Cyber Policy Center (2026): DigiChina & Mercator Institute for China Studies (2026): Search Results "Cyber" & The Record (2026): China News & Margin Research (2026): Resources & Intrusion Truth (2026) & Natto Thoughts (2026): i-SOON Leaks

34 Huseyin Can Yuceel (2026): Chinese Threat Actors: What Defenders Need to Know & Orange Cyberdefense (2026): The hidden network – How China unites state, corporate, and academic assets for cyber offensive campaigns

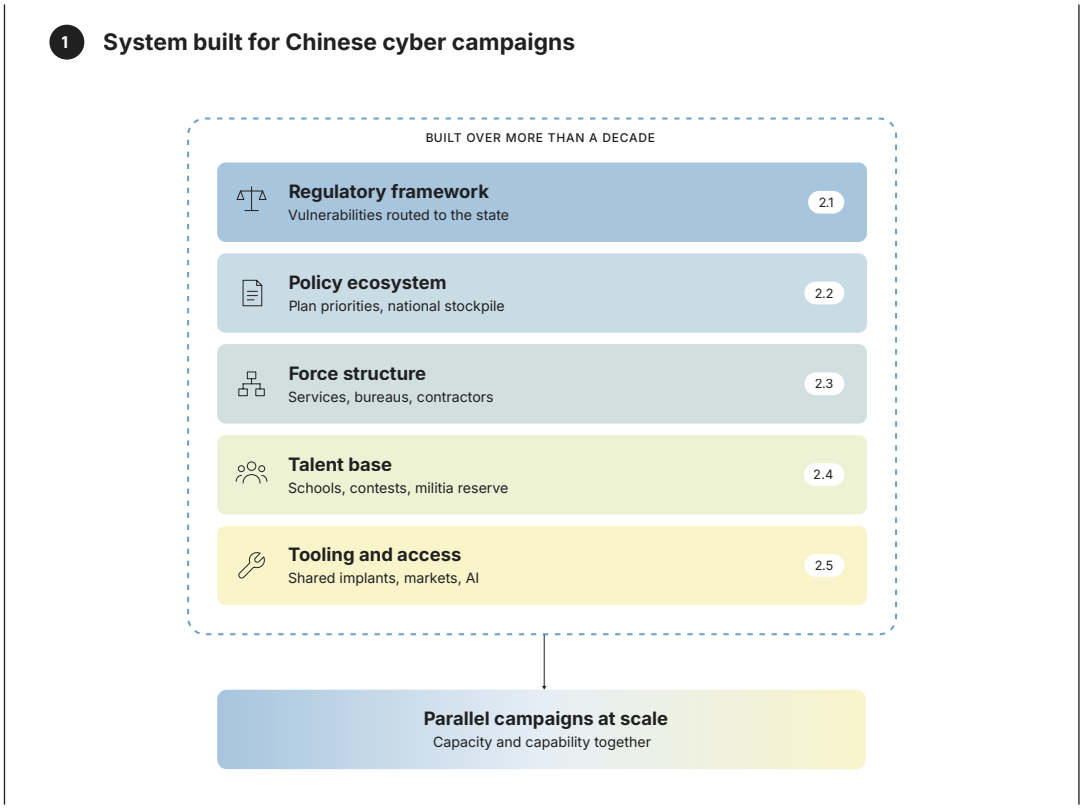


Figure 1. System built for Chinese cyber campaigns.

2.1 Regulatory Framework

Since 2017, the PRC has built a broad body of cyber and data law. The Cybersecurity Law, in force since June 2017, sets out the basic security obligations of network operators. The Data Security Law and the Personal Information Protection Law followed in 2021, giving the state far-reaching say over how data is classified, stored, and transferred abroad.[35] Much of this framework governs the domestic digital economy. For cyber operations, the provisions that matter most are narrower: they decide who learns first about weaknesses in hardware or software, and who is allowed to know. Vulnerabilities in hardware or software that are unknown to the vendor or maintainer – so-called "zero-days"[36] – are essential to many higher-tier cyber operations, because no patches or mitigations exist for them at the time that they are first discovered by the threat actor and exploited.[37] Individually

35 Margin Research (2023): China's Cyber Laws and Regulations & DigiChina (2021): Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)

36 Sven Herpig (2024): Vulnerability Disclosure: Guiding Governments from Norm to Action – How to Implement Norm J of the United Nations Norms of Responsible State Behaviour in Cyberspace

37 verizon business (2026): 2026 Data Breach Investigations Report & Vectra AI (2026): Zero-day vulnerabilities explained: what they are, how they work, and how to defend against them

or chained, vulnerabilities are turned into exploits which, for example, allow initial access into targeted IT systems. A state that wants first access to the zero-days its researchers discover, and wants that research kept at home, must compel both. The PRC has done so.

The Regulations on the Management of Network Product Security Vulnerabilities (RMSV)[38], published in 2021 by the Cyberspace Administration of China (CAC), the Ministry of Public Security (MPS), and the Ministry of Industry and Information Technology (MIIT), require companies that supply network products to report vulnerabilities in those products to the MIIT within two days. Researchers who find vulnerabilities are only encouraged to report them to state platforms.[39] The RMSV rests on China's Cybersecurity Law[40] and operates within this wider framework – including the Data Security Law (DSL)[41] and the National Intelligence Law (NIL)[42] – that gives the state privileged access to vulnerability information and, in the case of the NIL, compels organizations and individuals to support intelligence work under penalty for non-compliance. The rules work in one direction. They pull vulnerability information toward the state and restrict its flow away from it: information about an undisclosed vulnerability may not be passed to any foreign party except the vendor, and publication ahead of a vendor patch requires the involvement of the MIIT and the MPS.[43] The law on guarding state secrets sits above both, since a vulnerability bearing on national security or national interests may be classified and withheld on that basis alone. The rules leave a researcher free to tell the vendor first, including a foreign one. In practice, doing so carries a cost. When an Alibaba Cloud researcher reported the Log4Shell vulnerability to the Apache Software Foundation in 2021 before informing the MIIT, the ministry suspended the company from its threat-information sharing partnership for six months.[44]

The reporting that the RMSV leaves voluntary for researchers is mandatory at one of the main venues where they find and demonstrate vulnerabilities:

---

38 China Law Translate (2021): Provisions on the Management of Network Product Security Vulnerabilities

39 Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities

40 Rogier Creemers, Graham Webster, and Paul Triolo (2018): Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)

41 China Law Translate (2021): Data Security Law of the PRC

42 China Law Translate (2018): PRC National Intelligence Law (as amended in 2018)

43 Margin Research (2023): China's Cyber Laws and Regulations

44 South China Morning Post (2021): Apache Log4j bug: China's industry ministry pulls support from Alibaba Cloud for not reporting flaw to government first & China Daily (2021): Sources: MIIT suspends Ali Cloud partnership

hacking competitions. In 2018, the Chinese government issued a regulation, commonly rendered as "Regulating the Promotion of Cybersecurity Competitions"[45], that effectively barred its researchers from traveling abroad to take part in contests such as Pwn2Own[46] and required vulnerabilities found in domestic competitions to be reported directly to the relevant government departments. As a consequence, Chinese teams – for example from the cybersecurity company Qihoo 360 – shifted their participation to the China-based Tianfu Cup, a competition "designed as a Chinese version of Pwn2Own".[47] To win these competitions, a vulnerability must already be turned into a functional exploit, which places the output closer to weaponization for any threat actor that gains access to it. The same firm now credits much of that work to AI. In 2026 it reported that a multi-agent vulnerability discovery system had found close to 1,000 previously unknown flaws and had helped it take first place at the revived Tianfu Cup, although some of its individual claims have been disputed.[48] The redirection concerns exploit contests. Chinese teams still take part in capture-the-flag contests abroad, but working exploits against real products are now demonstrated at home, where they stay within the state's reach.[49] There is evidence of where they go next. An iPhone exploit that won the 2018 Tianfu Cup was used against Uyghurs within months,[50] and chats in the leaked i-SOON files describe the ministry passing Tianfu Cup vulnerabilities each year to the provinces it considers strong.[51]

What had initially been an outward-facing talent culture – Chinese university teams repeatedly qualifying for the DEF CON capture-the-flag finals in Las Vegas – was deliberately redirected inward,[52] by keeping the pipeline's output, vulnerabilities and exploits, within the state's reach.

First access to newly discovered vulnerabilities and exploits is, in effect, legislated and stockpiled as a strategic resource. One assessment of the

45 Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities & Office of the Central Cyberspace Affairs Commission and Ministry of Public Security (2018): Notice on Regulating the Promotion of Cybersecurity Competitions

46 Scott Graham (2026): Pwn2Own Berlin 2026: On the Ground With TrendAI™ ZDI's Biggest AI Showdown Yet

47 Karen Chiu (2019): Chinese hackers break into Chrome, Microsoft Edge and Safari in competition

48 Eduard Kovacs (2026): Chinese Cybersecurity Firm's AI Hacking Claims Draw Comparisons to Claude Mythos

49 Eugenio Benincasa (2024): From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem

50 Patrick Howell O'Neill (2021): How China turned a prize-winning iPhone hack against the Uyghurs

51 HarfangLab (2024): A comprehensive analysis of I-Soon's commercial offering

52 Eugenio Benincasa (2024): From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem

regulatory framework puts the effect plainly: the 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".[53] Assessed from the outside, that perspective appears to be shared by the PRC's own policy-makers and decision-makers. The chief executive of Qihoo 360 has remarked that vulnerabilities are "important strategic resources [that] should stay in China".[54]

Regulation also gives the state a detailed map of the networks in China. The Cybersecurity Law's Multi-Level Protection Scheme, rebuilt as "MLPS 2.0" through national standards that took effect on December 1, 2019, requires every network operated in China to be graded according to its importance to national security, secured accordingly, and – above a certain criticality threshold – registered with the local Public Security Bureau and independently assessed.[55] Notably, it binds foreign-owned operations exactly as it binds domestic ones. On its own, MLPS is a defensive-compliance regime. The ministry that grades, registers, and inspects these networks, however, is the MPS – the same ministry that receives vulnerability reports under the RMSV and conducts law-enforcement and intelligence operations in the cyber domain against targets inside the PRC.[56] A rule obliging operators to hand the police a graded map of every significant network in the country widens the state's visibility into, and access over, the systems its operators may later be tasked against. MLPS gives the PRC visibility into what is deployed and where. Finding the vulnerabilities happens elsewhere.

The state's legal authority does not stop at visibility. In April 2023, the PRC amended its Counter-Espionage Law to let state security organs employ "technical investigative measures", and to order telecommunications operators and internet service providers to respond to espionage-related risks – including network attacks – by repairing vulnerabilities, halting transmission, deleting content, suspending services, removing applications, closing websites, and retaining the related records.[57] This amendment is best understood as the PRC's entry into active cyber defense: the technical response by a state to malicious cyber activity

53 Insikt Group (2025): China's Zero-Day Pipeline: From Discovery to Deployment

54 Karen Chiu (2019): Chinese hackers break into Chrome, Microsoft Edge and Safari in competition

55 China Law Translate (2026): Cybersecurity Law of the People's Republic of China (2026 revised version) & European Commission (2026): Trade barriers "Cybersecurity Multi-Level Protection Scheme" & Hunton (2018): China Publishes the Draft Regulations on the Classified Protection of Cybersecurity

56 Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities

57 China Law Translate (2023): Counter-espionage Law of the P.R.C. (2023 ed.)

directed at it.[58] It does two things. It gives the MSS a standing statutory basis for intrusive operations, and it adds a further compelled-cooperation lever over the private sector, alongside the obligations already imposed under the National Intelligence Law. The defensive framing does not fit what the amendment allows: intrusive technical measures carried out by an intelligence service under an elastic counter-espionage mandate are difficult to distinguish, in method or effect, from offensive operations. The Multi-Level Protection Scheme already requires networks to be graded and registered. Alongside those obligations, the amendment widens what the state may do inside the PRC's networks and whom it can compel to act.

2.2 Policy Ecosystem

The state's planning documents set the overarching direction and serve as broad targeting guidance: observed collection through cyber campaigns aligns closely with the published priorities of successive Five-Year Plans. The plans are not the only driver, though. Province-level priorities, geopolitical needs, and new technological, economic or political developments also shape what is targeted, and not every operation traces back to a plan.[59] The current Five-Year Plan (2026–2030) calls for integrating cybersecurity into "every layer of digital development" while accelerating the drive to become a "cyber superpower".[60]

The extension of the military-civil fusion strategy[61] to the cyber domain – underway since around 2017 – embeds the People's Liberation Army's (PLA) "military-civil fusion centres" inside cybersecurity firms, allowing military personnel to work alongside company staff and giving the state access to zero-day vulnerabilities, joint research labs, and privately run infrastructure.[62]

58 Sven Herpig (2023): Active Cyber Defense – Toward Operational Norms

59 Sveva Vittoria Scenarelli (2026): Understanding modern Chinese cyber operations means shifting from 'APT' to composite responsibility

60 Natto Team (2026): Cybersecurity Strategy in China's 15th Five-Year Plan

61 Elsa B. Kania and Lorand Laskai (2021): Myths and Realities of China's Military-Civil Fusion Strategy

62 Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities

With its "Delete America" program, the PRC also aims to replace foreign hardware and software across the state sector by 2027.[63] As domestic products displace Western ones in Chinese systems, a plausible secondary effect – marked here as an assessment, not a stated aim of the program – is an asymmetry in what exploitation costs. A flaw in Western software that Chinese operators exploit abroad is increasingly one the PRC no longer runs at home, so it can be used, and left to spread, without exposing Chinese systems to the same risk.[64] That does not make Chinese systems harder to attack overall. Adversaries will turn to the domestic replacements instead, and how secure those are remains an open question. The state does hold one advantage there: vendors operating in the PRC must report vulnerabilities in their products to the MIIT within two days, so flaws in the replacements reach the state first.[65]

For zero-days, the law creates the duty to report, and policy turns that duty into a supply chain. The China National Vulnerability Database of Information Security (CNNVD), managed by the MSS, and the parallel, CNCERT/CC-run China National Vulnerability Database (CNVD) route disclosed vulnerabilities into state hands. The CNNVD rewards compliance – for example, with payment and preferential access to government contracts – making disclosure both mandatory and materially profitable.[66] Around the CNNVD sits a widening network of technical support units – universities, state-linked labs, and cybersecurity firms formally enrolled to feed vulnerability research inward. Their number has grown from fifteen firms in 2016 to over 150 by 2023 and is still expanding.[67] Research estimates that the support units field at least 1,190 dedicated vulnerability researchers and pass to the MSS on the order of 1,955 vulnerabilities a year, roughly 141 of them critical.[68]

63 Reuters' Beijing and Shanghai newsrooms, Raphael Satter, and AJ Vicens (2026): Beijing tells Chinese firms to stop using US and Israeli cybersecurity software, sources say

64 Insikt Group (2025): China's Zero-Day Pipeline: From Discovery to Deployment & Thomas Reinhold (2024): Segmentierung des Cyberspace? Chinas und Russlands Decoupling-Bestrebungen und ihre Konsequenzen

65 China Law Translate (2021): Provisions on the Management of Network Product Security Vulnerabilities

66 Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities & Insikt Group (2025): China's Zero-Day Pipeline: From Discovery to Deployment & Eugenio Benincasa and Natto Team (2025): China's Vulnerability Research: What's Different Now?

67 Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities

68 Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities

A further central government policy aims to scale vulnerability discovery by automating it. Since 2017, the PRC has run a series of government-backed "Robot Hacking Games"[69] – competitions modeled on the DARPA Cyber Grand Challenge[70] and aimed explicitly at advancing the automated discovery, patching, and exploitation of software vulnerabilities, with the PLA taking an increasing role in hosting them. Their stated purpose is to raise the scale and pace at which vulnerabilities can be found.

Disclosure policy is only one intake for vulnerabilities and exploits. Alongside it, the central government has organized acquisition. Since around 2016, the PRC has turned the regional market in zero-day vulnerabilities into a funnel channeling offensive capability toward its military and intelligence services. This policy relies on decentralized contracting that shortens acquisition cycles and extends an exploit's useful life through additional resourcing and reuse as known vulnerabilities, so-called n-days.[71] Parallel contracting of this kind is a scaling mechanism – many buyers and many suppliers transacting at once multiply throughput in a way a single centralized procurement office could not. A drawback is the higher likelihood of operations being burned, because the underlying vulnerabilities and exploits have often just become n-days through parallel procurement and deployment. This favors scale over persistence and accepts higher risk for potentially higher returns.

Where the vulnerabilities end up shows what the system is for. The RMSV pushes vulnerability reports to the MIIT before a patch exists. The ministry's platform then shares that data onward to CNCERT/CC and the MPS and, through the CNVD's onward distribution, to entities with offensive missions in addition to the MPS.[72] Recipients include the Beijing office of the MSS's 13th Bureau, Beijing TopSec – a contractor of the PLA – and a Shanghai Jiao Tong University center engaged in advanced-persistent-threat attack-and-defense research.[73] Once received by the MSS, the vulnerabilities are "almost certainly evaluated

69 Dakota Cary (2021): Robot Hacking Games – China's Competitions to Automate the Software Vulnerability Lifecycle

70 Defense Advanced Research Projects Agency (undated): CGC: Cyber Grand Challenge

71 Winnona DeSombre Bernsen (2025): Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace & Sven Herpig (2024): Vulnerability Disclosure: Guiding Governments from Norm to Action – How to Implement Norm J of the United Nations Norms of Responsible State Behaviour in Cyberspace

72 Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities & China Law Translate (2021): Provisions on the Management of Network Product Security Vulnerabilities

73 Dakota Cary and Kristin Del Rosso (2023): Sleight of hand: How China weaponizes software vulnerabilities

for offensive use", a reading grounded in the documented 2017 finding that the CNNVD withheld high-criticality entries from publication until an operation was burned, then disclosed them and moved on.[74]

Independent analysis sees the same trend: support units multiplying, public disclosure volumes falling, and competition results going dark together suggest a state that increasingly stockpiles vulnerabilities and weaponizes them selectively.[75] The supply chain runs from private discovery to operational use, under state control. **These policies produce a multi-tiered system of vulnerability and exploit handling. On one side, vulnerabilities are funneled into the government from researchers and companies, stockpiled, and carefully evaluated for targeted use. On the other side, vulnerabilities and exploits are purchased from the market for parallel deployment at scale, even when already degraded to n-days. The two policies converge on the same end by producing a deep and continuously replenished national stock of exploitable vulnerabilities.**

The record shows both tiers working on the same flaws, in two patterns. In the first, a vulnerability is used quietly and selectively before several groups exploit it at scale around the time of the patch. That happened with Microsoft Exchange in 2021, and again with SharePoint in 2025, when an initial round of targeted intrusions was followed by at least three China-based groups compromising an estimated 400 organizations.[76] In the second, several groups use the same exploit at the same time from the start. In September 2026, two Chinese groups launched phishing campaigns within a day of each other using an identical exploit chain against Chrome and Windows, aimed at a flaw whose fix had reached Chromium's public code but not yet the released browser.[77]

74 Priscilla Moriuchi and Bill Lad (2017): China's Ministry of State Security Likely Influences National Network Vulnerability Publications

75 Insikt Group (2025): China's Zero-Day Pipeline: From Discovery to Deployment

76 ESET Research (2021): Exchange servers under siege from at least 10 APT groups & Ryan Gallagher (2025): Tally of Microsoft Victims Surges to 400 as Hackers Exploit SharePoint Flaw

77 Ankur Saini, Conor Quigley, Sean Koessel, Steven Adair, and Tom Lancaster (2026): Mind the (Patch) Gap: Multiple Chinese Threat Actors Chain 0-day Exploits in Chrome & Windows

2.3 Force Structure

The PRC's force structure is organized to run all of this in parallel. Most PRC cyber operations observed abroad are assessed to run through the MSS, and much of that activity through its provincial bureaus.[78] US indictments and allied advisories have tied individual groups to individual bureaus – APT40 to Hainan, APT26 to Jiangsu, APT31 to Hubei – and operators charged in 2025 were said to act on tasking from the Shanghai bureau. Targeting often follows the priorities of the province, such as maritime technology in Hainan and aerospace in Jiangsu. Since reforms in 2016 and 2017, however, the central ministry has decided whom the bureaus employ, what they spend, and how they are supervised and tasked.[79] Execution is not confined to the province that orders it. Where bureaus once worked mainly through front companies in their own province, a maturing market now lets commercial firms take work from bureaus across provincial lines, so that provincially tasked operations can run at close to national scale.[80] **Tasking is spread across the provinces, while authority over the bureaus doing the tasking sits at the center.**

The military side has been rebuilt as well.[81] In its 2024 military reform, the government dissolved the Strategic Support Force (PLASSF) and stood up a standalone Cyberspace Force (CSF) alongside a new Information Support Force (ISF), with the Cyberspace Force making its public debut in April 2024.[82] The Dutch military intelligence service – the same agency that assesses Chinese offensive capability as roughly on par with the United States – ties the reorganization directly to performance, judging that it enabled "Chinese [threat actors] in 2025 to continuously adapt their tooling and infrastructure".[83] The reform also shows how the old structure had worked. Reporting on the reform assesses that the space, cyberspace, and communications elements had been pursuing their functions with considerable independence from the staff of the

78 Natto Thoughts (2025): The Many Arms of the MSS: Why Provincial Bureaus Matter in China's Cyber Operations

79 Natto Thoughts (2025): The Many Arms of the MSS: Why Provincial Bureaus Matter in China's Cyber Operations

80 Eugenio Benincasa (2026): Provincial Tasking, Cross-Provincial Execution: A Case-Based Look at How China Scales Cyber Operations

81 Dave Aitel, Sophia d'Antoine, Winnona DeSombre, Isabella Garcia-Camargo, Ian Roos, Nicholas Rostow, Jonathan Smith, Alison Strongwater, Abraham Wagner, and JD Work (2022): China's Cyber Operations The Rising Threat to American Security

82 Kieran Green (2025): Mobilizing Cyber Power: The Growing Role of Cyber Militias in China's Network Warfare Force Structure

83 Alexander Martin (2026): China's cyber capabilities now equal to the US, warns Dutch intelligence

force above them, and that the response was to dissolve the coordinating body instead of strengthening it, placing its three components directly under the Central Military Commission.[84] The military structure therefore follows the same pattern as the security services: tasking concentrated at the top, execution dispersed below it.

The reform also coincided with an investigation reaching the force's own commander, who had not appeared in public since mid-2023, at a time when corruption proceedings were affecting other parts of the military.[85] The reporting does not establish a connection between the two, and the rationale for the reform has not been made public. What can be observed is the timing: disciplinary attention reached the top of the military cyber structure during the same period in which debarment proceedings were reaching the contractors below it.

Around the professional military core sits a deliberately widened reserve. A study about the PRC's cyber militias describes a decade-long reform that moved them "from a peripheral asset into a strategically relevant component" of PLA cyber architecture: paramilitary units of civilian volunteers, raised by state-owned enterprises, universities, and technology firms "under the dual leadership of local governments and the PLA", and overseen through the National Defense Mobilization Commission.[86] Because these units also draw on people who already hold some offensive expertise, they let the PLA expand capacity at short notice on a scale uniformed forces alone could not easily reach. The reserve is real, but coordination and mobilization are inconsistent. In one case, a local armed-forces department could barely enlist twenty people, which shows that the reserve is strong in some places and thin in others.[87]

Beneath both the security services and the military sits the same layer: the contractors. Leaks about the firm i-SOON, also trading as Anxun Information Technology, became public in February 2024. Together with the subsequent

84 J. Michael Dahm (2024): A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force & J. Michael Dahm (2024): China C4ISR and Counter-Intervention

85 J. Michael Dahm (2024): A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force & J. Michael Dahm (2024): China C4ISR and Counter-Intervention

86 Kieran Green (2025): Mobilizing Cyber Power: The Growing Role of Cyber Militias in China's Network Warfare Force Structure

87 Kieran Green (2025): Mobilizing Cyber Power: The Growing Role of Cyber Militias in China's Network Warfare Force Structure

US indictment, the leaks give the clearest public picture of the scale.[88] A single firm worked with at least 43 separate MSS and MPS bureaus across 31 provinces and municipalities.[89] The firm's former website advertised work for the MPS, eleven provincial-level security bureaus, and some forty municipal public-security departments, selling "hack-for-hire" services and targeting platforms, subcontracting for other firms, and in some cases compromising targets on its own initiative before finding a buyer.[90] Its own presentation material advertised in-house APT units able to run several attack campaigns abroad at once.[91] The leak covers a single firm and may not be typical. Indictments, sanctions and further leaks describe the same setup at other firms, from Integrity Technology to Knownsec and the Nanjing and Zhengzhou companies discussed below. Provincial and municipal bureaus of the MSS and the MPS contract firms directly. Across the PRC's offensive cyber ecosystem, acquisition is decentralized, and "decentralization is a feature of the overall system rather than an exception".[92] Access to that work is regulated. State contracts require secrecy certification and certified-supplier status, and the military's procurement system can suspend a supplier from bidding or bar it for life.[93] What differs between the services is visibility. Suspensions from military procurement are published, which is why the debarments discussed in 3.2 can be observed at all, while contracting by the security services rarely becomes visible outside leaks and indictments.[94] **The execution layer is thus partially outsourced to a market of private contractors, not run as a single chain of command from the central government.**

88 Bundesamt für Verfassungsschutz (2024): BfV CYBER INSIGHT - The i-Soon-Leaks: Industrialization of Cyber Espionage (Part 1) & United States Attorney's Office (2025): 10 Chinese Nationals Charged With Large-Scale Hacking Of U.S. And International Victims On Behalf Of The Chinese Government

89 United States Attorney's Office (2025): 10 Chinese Nationals Charged With Large-Scale Hacking Of U.S. And International Victims On Behalf Of The Chinese Government & Federal Bureau of Investigation (2025): Beijing Leveraging Freelance Hackers and Information Security Companies to Compromise Computer Networks Worldwide

90 Frank Bajak and Dake Kang (2024): Leaked hacking files show Chinese spying on citizens and foreigners alike & United States Attorney's Office (2025): 10 Chinese Nationals Charged With Large-Scale Hacking Of U.S. And International Victims On Behalf Of The Chinese Government & Simon Sharwood (2024): Giant leak reveals Chinese infosec vendor I-Soon is one of Beijing's cyber-attackers for hire

91 Bundesamt für Verfassungsschutz (2024): BfV Cyber Insight – The i-Soon Leaks: Industrialization of Cyber Espionage, Part 1: Organization and methods of i-Soon APT units

92 Winnona DeSombre Bernsen (2025): Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace

93 Orange Cyberdefense (2026): The hidden network – How China unites state, corporate, and academic assets for cyber offensive campaigns & Eduard Kovacs (2026): China's Top Cybersecurity Firms Hit by Mounting Military Procurement Bans

94 Eugenio Benincasa and Natto Team (2026): China's Cybersecurity Powerhouses Face PLA Procurement Curbs & Eduard Kovacs (2026): China's Top Cybersecurity Firms Hit by Mounting Military Procurement Bans

That market is a dense, self-dealing web of firms, partially staffed by the same generation of former patriotic hackers – the so-called "Red 40" – who founded China's commercial security industry.[95] Chengdu 404, a company linked to APT41,[96] had a documented business relationship with i-SOON and saw three of its own personnel indicted in the United States in 2020.[97] Integrity Technology – a large Beijing contractor with ties to state security and public security bureaus, sanctioned by the United States in January 2025 as the entity supporting the Flax Typhoon intrusions and the operator of a botnet[98] – was simultaneously named in the i-SOON leaks as one of that firm's chief competitors and clients.[99] Integrity Technology also builds the PRC's cyber ranges and co-organizes the Matrix Cup, giving it first sight of the talent pipeline.[100] The pattern reaches the listed majors, not only the mid-tier contractors. Documents attributed to VenusTech – a publicly traded security vendor with long-standing ties to the PLA – surfaced for sale in 2025 and appeared to show offensive services sold to government customers: spreadsheets of collection targets and already-compromised organizations, and, in one line item, a monthly-billed feed from a foreign legislature's mail server, with victims spanning several jurisdictions.[101] The same people cycle between competitors, clients, and subcontractors. This multiplies the state's capacity and spreads accountability across many nominally private companies. It also makes any single attribution by a foreign government look like the act of a rogue firm, when it is a feature of how the system runs.

95 Eugenio Benincasa (2025): Before Vegas: The "Red Hackers" Who Shaped China's Cyber Ecosystem

96 National CSIRT-CY (2020): U.S. charges Chinese Winnti hackers for attacking 100+ companies (APT41)

97 U.S. Department of Justice (2020): Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally & Natto Team (2023): i-SOON: Another Company in the APT41 Network & Mudit Bansal (2024): Chinese APT Tactics and accesses uncovered after analyzing the I-SOON repository

98 Jonathan Greig (2025): US sanctions prominent Chinese cyber company for role in Flax Typhoon attacks

99 Jonathan Greig (2025): US sanctions prominent Chinese cyber company for role in Flax Typhoon attacks & U.S. Department of the Treasury (2025): Treasury Sanctions Technology Company for Support to Malicious Cyber Group & Eugenio Benincasa (2025): The 40 'Red Hackers' Who Shaped China's Cyber Ecosystem

100 Jonathan Greig (2025): US sanctions prominent Chinese cyber company for role in Flax Typhoon attacks

101 SpyCloud Labs Research Team (2025): State Secrets for Sale: More Leaks from the Chinese Hack-for-Hire Industry & Rahul Prakash (2013): China and Cyberspace

2.4 Talent Base

The people came before the institutions, and the state built the institutions around them. The PRC's contemporary offensive-cyber workforce traces to the "red hackers", or Honkers, of the late 1990s and 2000s – an independent, patriotic-hacker community that operated on its own initiative but frequently aligned with state interests against foreign targets.[102] Its most prominent members, the so-called "Red 40", professionalized as commercial incentives emerged, taking senior security roles at Baidu, Alibaba, Tencent, and Huawei, founding or leading firms such as VenusTech, TopSec, NSFOCUS, and Knownsec, and standing behind contractors such as i-SOON and Integrity Technology.[103] This is not only history: the operators, tool developers, and company managers behind several PRC-based APT groups trace back to this same community.[104] As a result, **the central government did not have to manufacture a hacking culture. It needed to ensure that the culture worked in the right direction and to provide incentives through regulation, policy, or structure where needed.**[105]

What began as patriotic improvisation is now an academic pipeline organized by the state, which combines offensive training with AI more closely than most Western programs do. Since 2017, the Ministry of Education (MoE) and the CAC have certified eleven "World-Class Cybersecurity Schools", eight of which build artificial-intelligence and machine-learning coursework into their cybersecurity degrees.[106] The offensive orientation is written into the curriculum standard: the MoE's 2022 white paper on cybersecurity talent defines "attack-and-defence live-fire capabilities" as a core competency, and some of the eleven certified schools

102 Eugenio Benincasa (2024): From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem

103 Eugenio Benincasa (2024): From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem

104 Eugenio Benincasa (2025): The 40 'Red Hackers' Who Shaped China's Cyber Ecosystem

105 Not all of China's hacker community fits this description. The state has also used criminal prosecution and social pressure against hackers who were not "patriotic", or who turned against the government, and has pushed them to the margins. That side of the record is thinly documented and lies outside the scope of this paper. The legal instrument is readily available, since unauthorized intrusion into computer systems is a criminal offense under Chinese law. See Margin Research (2023): China's Cyber Laws and Regulations.

106 Dakota Cary (2021): China's CyberAI Talent Pipeline & Ben Murphy (2021): Notice on the Publication of Management Methods for the Demonstration Project for Building World-Class Cybersecurity Colleges [Translation]

helped author it.[107] Several also sit close to operational activity, combining education, hands-on practice, and career placement in ways that support the security services, with schools such as Xidian, Hainan, and Southeast University cited as examples.[108]

The National Cybersecurity Talent and Innovation Base in Wuhan houses a National Cybersecurity School alongside two government-focused laboratories, one of them an Offense-Defense Lab, and hosts cyber ranges supplied by private contractors.[109] The base is tied to both the MSS and the PLA, and its government laboratories are assessed to conduct research for state use.[110] The orientation shows at the research frontier too. Since 2021, at least six universities with links to known state-sponsored operations have carried out cutting-edge AI research, in an ecosystem where the AI and offensive-cyber industries are closely connected, and high-end science and engineering schools are reported to steer graduates toward applied offensive projects.[111] **The state has built a system of schools, laboratories, and ranges in which attacking is taught, funded, and rewarded. It trains talent as well as recruiting it.**

The competition circuit turns that talent into identified, ranked, and recruitable operators. Talent identification has become systematic and data-driven: candidates are ranked by their performance in contests, their bug-bounty earnings, and the number of vulnerabilities they submit – clearer signals of skill and motivation than the old informal networks offered.[112] The domestic competitions used for this

107 Eugenio Benincasa and Natto Team (2025): China's Cybersecurity Companies Advancing Offensive Cyber Capabilities Through Attack-Defense Labs & Ben Murphy (2023): 2022 White Paper on the Live-Fire Capabilities of Cybersecurity Talents: Attack and Defense Live-Fire Capability Edition [Translation]

108 Dakota Cary (2022): Dakota Cary's Testimony Before the U.S.-China Economic and Security Commission

109 Dakota Cary (2021): China's National Cybersecurity Center – A Base for Military-Civil Fusion in the Cyber Domain & Dakota Cary (2023): China's Offense and Defense Talent & BaiduWiki (undated): Wuhan Cybersecurity University & Dakota Cary and Jennifer Melot (2021): National Cybersecurity Center Map

110 Dakota Cary (2021): China's National Cybersecurity Center – A Base for Military-Civil Fusion in the Cyber Domain & Dakota Cary (2022): Dakota Cary's Testimony Before the U.S.-China Economic and Security Commission & Dakota Cary and Eugenio Benincasa (2024): Capture the (red) flag: An inside look into China's hacking contest ecosystem & Dakota Cary (2021): Academics, AI, and APTs How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research

111 Dakota Cary and Eugenio Benincasa (2024): Capture the (red) flag: An inside look into China's hacking contest ecosystem & Dakota Cary (2021): Academics, AI, and APTs How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research

112 Eugenio Benincasa (2024): From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem & Dakota Cary and Eugenio Benincasa (2024): Capture the (red) flag: An inside look into China's hacking contest ecosystem

identification and recruitment include the Tianfu Cup, now under MPS lead[113], the Wangding Cup, used by the MPS to identify potential recruits for its Cybersecurity Thousand Talents Program[114], the Matrix Cup, whose inaugural 2024 event had a prize pool roughly double that of Pwn2Own[115], and the QiangWang Cup, co-hosted by the PLA Information Engineering University and co-guided by the CAC.[116] Because winning normally requires turning a vulnerability into a working exploit, these contests select directly for offensive skill, and they are woven into the same web as the contractors. Together with the automated "Robot Hacking Games" and the 2018 ban on competing abroad, the contests are how the PRC finds offensive talent, and it keeps them at home on purpose.

The PRC does not only employ or contract this talent. It also holds it in reserve. The same pool of industry and university expertise is organized into paramilitary cyber militias – volunteer units raised from state-owned enterprises, universities, and technology firms – that let the state surge skilled manpower on demand.[117] **This pipeline does double duty: it trains and retains talent in the firms and government services that run day-to-day operations, and it fills a mobilizable reserve the state can call up.**

2.5 Tooling And Access

A system built for volume also has to make each operation cheaper, and this is where the PRC's system is changing fastest. At the top end, AI is becoming part of the operation. By late 2025, a Chinese state-linked group had wired a commercial AI coding model into an autonomous attack framework. According to a vendor assessment, the framework ran roughly 80 to 90 percent of the tactical work across the intrusion chain[118] – against some thirty technology, finance, chemical, and government targets – with human operators stepping in only at a handful

113 Eugenio Benincasa (2026): The Tianfu Cup Returns Under MPS Leadership as AI Takes Center Stage

114 Dakota Cary and Eugenio Benincasa (2024): Capture the (red) flag: An inside look into China's hacking contest ecosystem

115 Winnona DeSombre Bernsen (2025): Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace & Eduard Kovacs (2024): $2.5 Million Offered at Upcoming 'Matrix Cup' Chinese Hacking Contest

116 Natto Thoughts (2026): Hacking Contests & Training & Dakota Cary and Eugenio Benincasa (2024): Capture the (red) flag: An inside look into China's hacking contest ecosystem

117 Kieran Green (2025): Mobilizing Cyber Power: The Growing Role of Cyber Militias in China's Network Warfare Force Structure & Devin Thorne (2025): China's Militia Forces Train to "Get Strong" in the New Era

118 Lockheed Martin (undated): Cyber Kill Chain

of decision points.[119] The same shift shows at the more institutionalized level: at the 2026 Tianfu Cup, around half of one leading firm's landed vulnerabilities relied on AI-assisted discovery and exploitation, with AI described in the firm's own account as having moved "from an auxiliary tool to the core engine of vulnerability discovery".[120] Of course, these are the most advanced cases, not the typical ones. **But the direction is clear: Chinese threat actors are building AI into the intrusion chain as a standing capability.**

Below that leading edge sits a mature market in shared tooling, and here the looseness first shows in the tools themselves. Capability is built once and reused across groups. ShadowPad, a backdoor that may have originated with the contractor Chengdu 404, whose personnel were later indicted for activity attributed to APT41, went from about 2019 to groups linked to the MSS and to several PLA theater commands. Its seller restricted it to a small circle of customers, unlike PlugX, which was sold openly.[121] A tool built once and sold to several users saves the state effort, but it also makes attribution and clean-up harder.

Access changes hands more readily than tools. The i-SOON leaks and the subsequent US indictment reveal a contractor selling not only intrusion services but the proceeds of intrusions already carried out – access to compromised mailboxes and networks, extracted data, and ready-made targeting platforms – to a roster of Chinese government clients.[122] Apart from known vulnerabilities, stolen credentials are consistently among the leading vectors for initial compromise,[123] and the same contractor offered its government clients tools to crack passwords and get around multi-factor authentication.[124] **The pipeline therefore supplies vulnerabilities and exploits, tools for stealing credentials, and ready-made access, lowering the barrier for any operator the state chooses to task.**

---

119 Anthropic (2025): Disrupting the first reported AI-orchestrated cyber espionage campaign

120 Eugenio Benincasa (2026): Chinese Firm Claims AI-Driven Bug Discovery Near Claude Mythos Scale

121 Yi-Jhen Hsieh and Joey Chen (2021): ShadowPad | A Masterpiece of Privately Sold Malware in Chinese Espionage & U.S. Department of Justice (2020): Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally & National CSIRT-CY (2020): U.S. charges Chinese Winnti hackers for attacking 100+ companies (APT41) & Sophos Counter Threat Unit Research Team (2025): ShadowPad Malware Analysis

122 U.S. Department of Justice (2025): Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns & J. Edward Moreno (2024): China's Hacker Network: What to Know & Raphael Satter (2025): US indicts slew of alleged Chinese hackers, sanctions company over spy campaign

123 verizon business (2026): 2026 Data Breach Investigations Report & Vectra AI (2026): Zero-day vulnerabilities explained: what they are, how they work, and how to defend against them

124 U.S. Department of Justice (2025): Sealed Indictment (24 Crim 687), United States v. Wu Haibo et al.

Because of that market, tools and exploits regularly pass between groups. The PlugX family shows the range: a single lineage that runs from disciplined, target-selective tasking against hard diplomatic targets at one end to a self-propagating variant that spread across millions of machines at the other.[125] Exploits often travel the same way, from careful targeting to indiscriminate use, sometimes within days. Once the patch for the Hafnium/ProxyLogon flaw was released, a compromise the MSS had first held closely became "open season", spreading across Chinese state and criminal threat actors alike.[126] The same diffusion is built into how the market is tiered: less-capable "D-teams" inherit access and tooling once the elite "A-teams" are done with it.[127] **Proliferation is therefore part of how the system works. Shared tools and inherited access blur the line between elite tasking and freelance opportunism, and repeatedly expose operations that a tighter model would keep quiet for longer.**

2.6 System Findings

Read together, the five layers in Figure 1 feed one another. The regulatory framework routes newly found vulnerabilities toward the state, and the policy ecosystem turns that duty into a supply chain, with a stockpile for selective use and a market for use at scale. The talent base supplies the people. They work for the contractors and for the firms and universities that feed the state's vulnerability databases, they make up the militia reserve, and the contests that rank them also produce working exploits that stay in the country. The market in tools and access lowers the cost of each operation for whichever operator is tasked. Together, the layers work like a production line, from finding vulnerabilities to using them at scale, and AI is beginning to run parts of that line continuously (2.5, 5.3). All of it comes together in the force structure, where security bureaus, military cyber forces and their contractors run the operations. The same organizations recur across the layers. Integrity Technology operated a botnet, supported intrusions, builds the PRC's cyber ranges and co-organizes a talent contest. i-SOON worked for dozens of security bureaus and sold access, data and hacking platforms. TopSec, one of the firms the "Red 40" founded or led, is a PLA contractor and receives vulnerability data from the state.

---

125 U.S. Department of Justice (2025): Justice Department and FBI Conduct International Operation to Delete Malware Used by China-Backed Hackers & Mark Kelly, Georgi Mladenov, and the Proofpoint Threat Research Team (2026): I'd come running back to EU again: TA416 resumes European government espionage campaigns

126 Shaun Waterman (2026): American Hackers-for-Hire Proposal Sparks Heavy Criticism

127 Winnona DeSombre Bernsen (2025): Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace & Ryan Gallagher (2025): Microsoft Hack Hits Hundreds of Firms, Agencies as Damage Spreads

Two findings follow for affected states. First, the system replenishes itself: the stock of vulnerabilities is refilled continuously, the talent pipeline keeps supplying operators, and the market keeps supplying tools and access, partly from what earlier operations leave behind. Action against a single group, firm or tool leaves the rest of the system in place. Pressure reaches further at points that many operators share, such as commercial infrastructure and the firms that supply it (6.2). Second, control is held at the core – the rules, the vulnerability pipeline and authority over the bureaus – and looseness shows first at the edge, where execution is delegated to contractors and bought on a market.

2 **The PRC cyber campaign ecosystem**

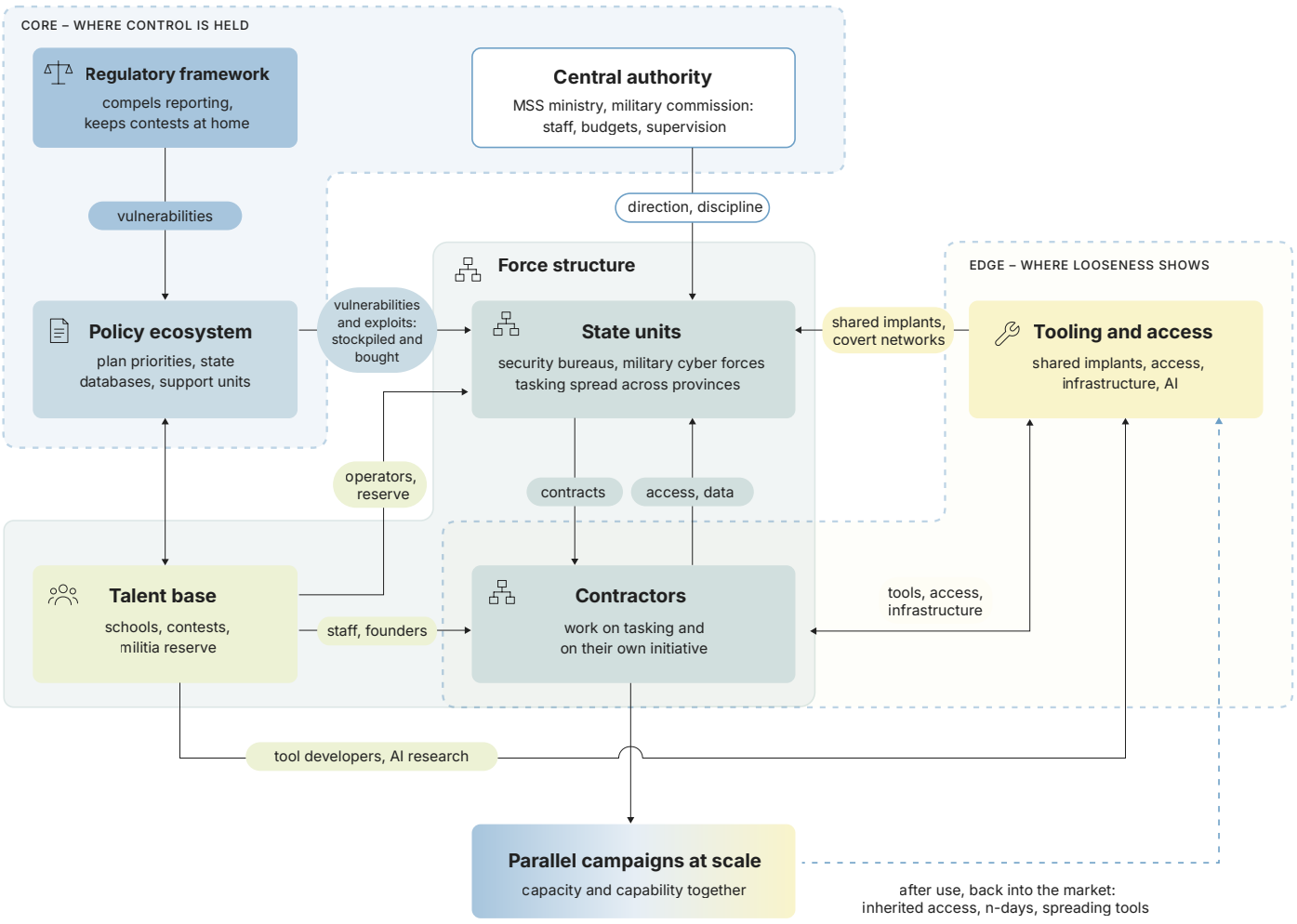


Figure 2. The PRC cyber campaign ecosystem.

3. Control: Bounded, Not Lost

Control over the PRC's cyber campaigns is bounded, not lost. The looseness has limits: the central government lets its operators work loosely, within a lower limit it enforces and an upper limit that has so far held. The lower limit is where it steps in. It corrects its operators when their conduct touches the state's own interests, as with misconduct in bidding for military contracts, and it corrected how they operate once, in 2015, when commercial cyber espionage strained the relationship with the United States (3.2). The upper limit is a ceiling. No PRC campaign has yet been aimed at disrupting the operation of foreign critical infrastructure, even where access is in place, although that limit has not been tested (3.3). Between the two limits, contractors act on their own initiative, espionage blends with crime, and tools are shared. The state tolerates this looseness (3.1). Not lost means that the state keeps the means to correct its operators, and uses them when its own interests are at stake.

The system set out in Chapter 2 was built over more than a decade, for volume and, increasingly, for capability that is able to rival the most advanced state programs.[128] Looseness in a system the state has invested in this heavily is not necessarily a sign of failure. The contractor opportunism, the spread of tools, and the noisy, attributable operations can be read in two ways. **On the one hand, the disorder is a real loss of control: the central government has built an ecosystem it can no longer adequately oversee, and operations run beyond what it intended or can discipline. On the other hand, it is a cost the central government has accepted – tolerating disorder at the operational edge as the price of speed, reach, and deniability, while retaining control where it matters most: the strategic direction and the capacity to discipline the operators and firms it relies on when it chooses to. The distinction carries a direct consequence for affected states: it determines whether these campaigns reflect the PRC losing its grip, which it may in time recover, or a policy it has chosen and sees no reason to change. The second calls for an answer from affected states.**

Choosing between the readings does not require settling whether the central government is "in control" in some absolute sense. No distributed system of this size operates under complete central command, and asked that way, the question looks for a level of control that probably no comparable state has. The more useful question is narrower and observable: how much looseness the central government tolerates before it intervenes to correct it.

128 Alexander Martin (2026): China's cyber capabilities now equal to the US, warns Dutch intelligence

This question connects directly to the seventh red flag of the companion framework *Assessing Irresponsibility in Cyber Operations,* which concerns operational control that is lacking or lost and identifies two triggers: control that is deliberately abandoned, and control that is unintentionally lost.[129] The PRC fits neither cleanly. Its delegation is deliberate and not abandoned – the central government has not stepped away from its operators – and the looseness, though real, does not amount to a loss of control. The reading Chinese practice supports lies between the two triggers: control that is bounded, and not lost. Figure 3 sorts the record by two questions: whether the conduct concerns how operators operate or how contractors do business, and whether it touches the state's own interests.

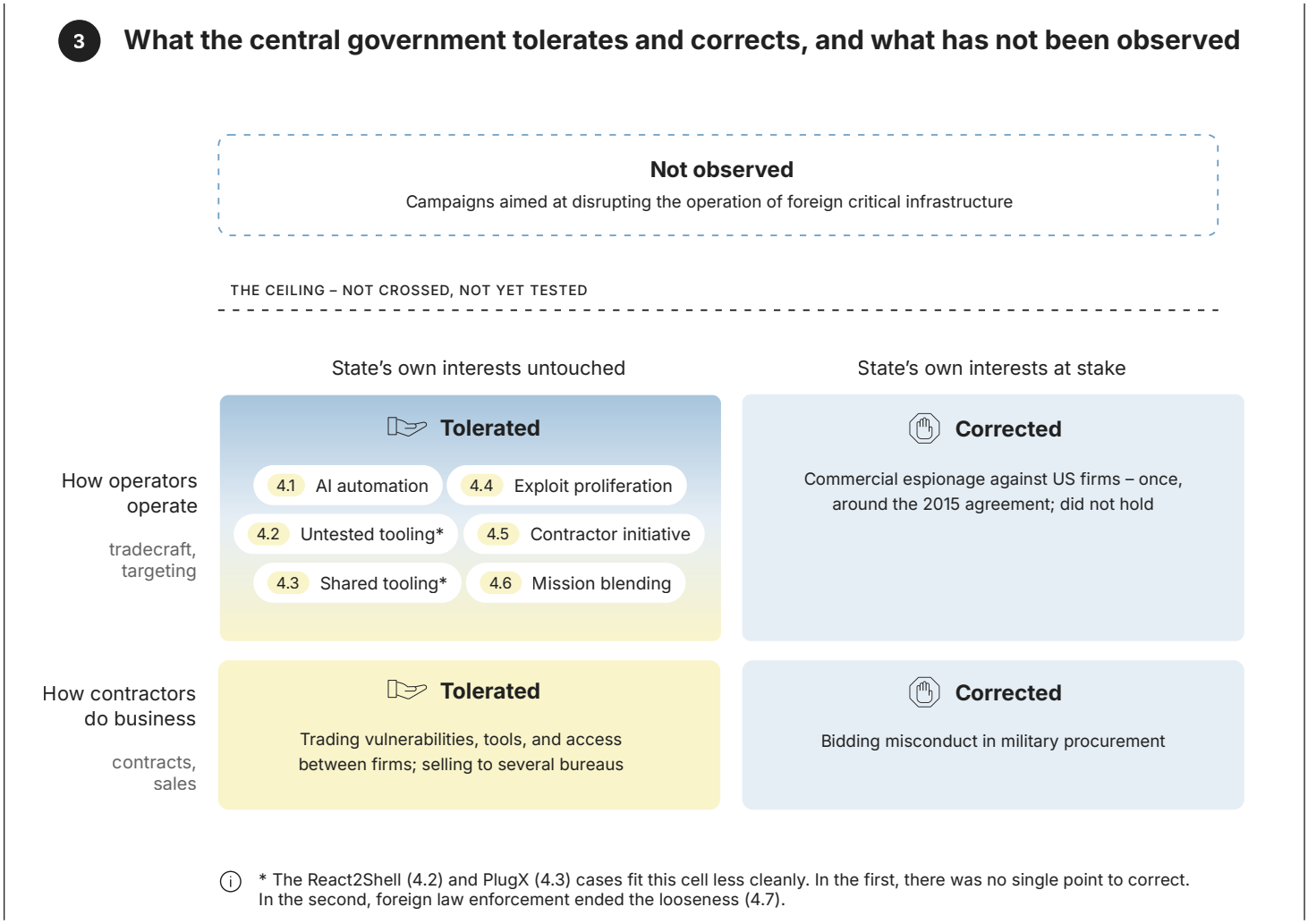


Figure 3. What the central government tolerates and corrects, and what has not been observed.

129 Sven Herpig (2025): Assessing Irresponsibility in Cyber Operations – A Guide for Operators and Decision-Makers in Times of Strategic Competition

3.1 Tolerated Looseness

Three patterns of tolerated looseness recur across the case record. In each, the state can see the looseness and leaves it in place.

The first is a set of commercial markets in the inputs to operations – initial access and tooling – that the central government sustains but does not individually task. Access is one such market: a contractor may compromise a target on its own initiative and seek a state buyer afterward, as the i-SOON record shows.[130] Infrastructure is another, one layer down. Covert networks are built and maintained by commercial firms and may be sold to several customers at once, so that a single vendor's network can sit beneath multiple unrelated operators and bureaus.[131] Court filings unsealed in August 2026 describe one such supplier. The Nanjing Xinjiuwei Network Technology Company provided infrastructure that hid the origin of cyber campaigns run by several actors, including the MSS and the PLA.[132] Access has become a trade in its own right. One MSS-linked operator has been assessed as conducting access operations specifically, exploiting newly disclosed vulnerabilities in security appliances and remote-access software at scale and then offering the resulting footholds for sale, including access to defense contractor appliances and government entities in the United Kingdom and Asia.[133] Integrity Technology built that split into its products. According to US authorities, one of its tools scanned networks for weaknesses that the company's customers would go on to use – among the targets a US power company, Japanese and Polish airports, and Taiwanese gas and power companies.[134] A second tool, delivered by phishing, opened victim networks to those customers or collected chosen files and sent them back to the company.[135] One party carries out the intrusion and another

130 United States Attorney's Office (2025): 10 Chinese Nationals Charged With Large-Scale Hacking Of U.S. And International Victims On Behalf Of The Chinese Government & Natto Thoughts (2026): i-SOON Leaks

131 Cybersecurity & Infrastructure Security Agency (2026): Defending Against China-Nexus Covert Networks of Compromised Devices

132 U.S. Department of Justice (2026): Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure & United States Attorney's Office (2026): Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure

133 Michael Raggi, Adam Aprahamian, Dan Kelly, Mathew Potaczek, Marcin Siedlarz, and Austin Larsen (2024): Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect & Sveva Vittoria Scenarelli (2026): Understanding modern Chinese cyber operations means shifting from 'APT' to composite responsibility

134 U.S. Department of Justice (2026): Justice Department and FBI Seize Vulnerability Scanning and Spear Phishing Tools Operated and Used by China-State Sponsored Hackers

135 U.S. Department of Justice (2026): Justice Department and FBI Seize Vulnerability Scanning and Spear Phishing Tools Operated and Used by China-State Sponsored Hackers

uses it: a division of labor along a supply chain. The court filings concerning Nanjing Xinjiuwei Network Technology Company also describe how such work is obtained. Employees of the company are said to include former members of the PLA, who are described as drawing on those relationships to win contracts and subcontracts supporting offensive operations.[136] **The state has not lost sight of a contractor that hires from the institution it supplies and wins work through those ties.** The filings establish this for one firm, and a single case does not show how common it is. Ties between the state and its suppliers are documented elsewhere in other forms: military-civil fusion centers place PLA personnel inside cybersecurity firms (2.2), and bureaus have worked through front companies of their own (2.3).

Firms that compete for the same state contracts also trade with one another, and reporting indicates that one contractor purchased a vulnerability affecting a messaging platform from a competitor for use in an intrusion campaign. Where such dealings break down, the parties have turned to the courts: a firm associated with APT41 brought an intellectual property claim against another contractor.[137] **Suppliers that trade with their competitors and take each other to court in China operate inside a commercial order.** That order also shows from the inside. Internal documents from the contractor Beijing Knownsec Information Technology, made public at the end of 2025, set out a firm organized like any other: an offensive research unit, a product development center converting research into deployable tooling, a data division maintaining breach archives and credential holdings, a division adapting the same products for military customers, and project managers running the work against delivery timelines.[138] Another disclosure followed in September 2026, when internal chat logs, a slide deck and illegally obtained data from a Zhengzhou firm became public.[139] Its customers included local police units across several regions of China. Demand for foreign intelligence reaches down to local police units, and the supply layer is organized to meet it. There have been four such disclosures in three years, and none has been followed by correction so far.

136 U.S. Department of Justice (2026): Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure & Sean Lyngaas (2026): US says Chinese hackers hit hospitals, NASA, Senate and more

137 Orange Cyberdefense (2026): The hidden network – How China unites state, corporate, and academic assets for cyber offensive campaigns & Winona Bernsen (2024): Same Same, but Different & Natto Team (2023): i-SOON: Another Company in the APT41 Network

138 Resecurity Cyber Threat Intelligence (2025): Knownsec Data Breach: A Trove of Espionage Tradecraft with an Insider Narrative & DomainTools Investigations (2026): THE KNOWNSEC LEAK: Yet Another Leak of China's Contractor-Driven Cyber-Espionage Ecosystem

139 Josh Chin, Gabriele Steinhauser, and Tripti Lahiri (2026): How a Chinese Hacking Firm Tapped AI to Supercharge Cyber-Spying

The second pattern is tolerated contractor opportunism and mission-blending. The boundary is porous in both directions: state-tasked actors mix espionage with financially motivated crime, as the activity associated with APT41 shows.[140] Running the other way, financially motivated groups have moved upward into state-style operations while continuing their criminal campaigns, as reported of Silver Fox since at least 2024.[141] Capability moves down into crime and up into state service, and the state corrects neither. Reporting on the relationship suggests why. Supervising organs are described as overlooking the criminal activity of groups they work with in exchange for cooperation in collection, and, in some cases, as using prior criminal conduct as leverage to secure that cooperation in the first place.[142] One indictment records the setup from the operator's side. One of the Chengdu 404 staff charged in 2020 claimed to be "very close" to the MSS, described the relationship as protection, including from the Ministry of Public Security, "unless something very big happens", and advised an associate not to "touch domestic stuff anymore".[143] On that account, not correcting is part of the deal.

Sharing between various threat actors extends to access already established. Vendor analysis of two PRC-sponsored groups describes established, persistent access to a compromised asset being passed from one to the other partway through an intrusion, so that a second operator enters an operation already under way and continues it.[144] The second operator skips reconnaissance and initial exploitation, and no single operator's actions explain the whole intrusion. Where two parties carry out an intrusion one after the other, responsibility can only be settled at the level of the system that allowed the handover.

---

140 Eugenio Benincasa (2026): Whack-a-Mole: How China's War on Cybercrime Pushed Fraud Offshore – and Ignited a U.S. Crackdown & U.S. Department of Justice (2020): Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally

141 Pierre Le Bourhis and Coline Chavane (2026): Silver Fox: The Only Tax Audit Where the Fine Print Installs Malware

142 Dave Aitel, Sophia d'Antoine, Winnona DeSombre, Isabella Garcia-Camargo, Ian Roos, Nicholas Rostow, Jonathan Smith, Alison Strongwater, Abraham Wagner, and JD Work (2022): China's Cyber Operations The Rising Threat to American Security & Adam Kozy (2022): Testimony before the U.S.-China Economic and Security Review Commission Hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States"

143 U.S. Department of Justice (2020): Indictment, United States v. Jiang Lizhi, Qian Chuan, and Fu Qiang

144 Michael Raggi, Adam Aprahamian, Dan Kelly, Mathew Potaczek, Marcin Siedlarz, and Austin Larsen (2024): Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect & Sveva Vittoria Scenarelli (2026): Understanding modern Chinese cyber operations means shifting from 'APT' to composite responsibility & Daniel Lunghi and Leon M Chang (2025): The Rise of Collaborative Tactics Among China-aligned Cyber Espionage Campaigns

The third pattern is the tolerated spread and loss of tools at the edge. This pattern concerns what happens to tools after they are used: once a tool is in the field, its spread is hard to control, and the state has let it spread. The pattern appears where a closely held vulnerability becomes generally exploited after disclosure, as in the ProxyLogon case,[145] and where a shared tool proliferates far beyond the operators who first fielded it, as in the PlugX lineage.[146]

The same pattern is recorded in government assessments rather than in vendor reporting alone. An advisory led by Australia's signals intelligence agency in July 2024, co-sealed by agencies from seven other states, sets out the tradecraft of a group assessed to receive its tasking from the MSS, and states the expectation that it will continue to adapt proof-of-concept code for newly disclosed "vulnerabilities within hours or days of public release".[147] Even the cover for state sponsorship is handled loosely. Thirteen front companies associated with a single MSS-linked cluster shared similar names and were registered by the same individuals or to the same addresses, which is what allowed them to be identified as a set.[148]

3.2 Selective Correction

Tolerating looseness does not mean ignoring it. What the central government tolerates has two observable limits, and these limits distinguish bounded delegation from lost control.

The lower limit shows what triggers correction: misconduct in bidding for contracts, not operational exposure. The debarments seen in the first half of 2026 corrected the books – contracting misconduct inside the ecosystem – but left the tradecraft untouched.[149] Independent assessments reach the same

145 Michael Heller (2021): MTR in Real-Time: Exchange ProxyLogon Edition

146 Shaun Waterman (2026): American Hackers-for-Hire Proposal Sparks Heavy Criticism & Mark Kelly, Georgi Mladenov, and the Proofpoint Threat Research Team (2026): I'd come running back to EU again: TA416 resumes European government espionage campaigns & U.S. Department of Justice (2025): Justice Department and FBI Conduct International Operation to Delete Malware Used by China-Backed Hackers

147 Cybersecurity & Infrastructure Security Agency (2024): People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action & Australian Signals Directorate (2024): PRC state-sponsored cyber group APT40's expanding tradecraft and tactics

148 intrusiontruth in Hainan (2020): What is the Hainan Xiandun Technology Development Company? & Orange Cyberdefense (2026): The hidden network – How China unites state, corporate, and academic assets for cyber offensive campaigns

149 Eugenio Benincasa and Natto Team (2026): China's Cybersecurity Powerhouses Face PLA Procurement Curbs & Eduard Kovacs (2026): China's Top Cybersecurity Firms Hit by Mounting Military Procurement Bans

point from outside. One finds that the PRC's contracting process "largely does not penalize organizations when they are caught or attributed", except where one company embarrasses the wider intelligence system. Another finds that the steady rise in public attribution has not prompted a basic rethink of how the model operates, and reads attribution as a cost to be managed and not as a binding constraint.[150] The public response points the same way. Attributions draw near-identical statements – that China "firmly opposes and combats cyber attacks and cyber theft in all forms" and that tracing the operations is "a complex technical issue" – and at times attacks on the credibility of whoever made them.[151] Neither changes how the operations are run.

Unauthorized intrusion into a computer information system is a criminal offense under Chinese law, as is impairing the functioning of one, and the criminal law can also reach conduct by Chinese nationals outside the mainland.[152] Contractual instruments run alongside the criminal ones. The certification and supplier status that state work requires (2.3) give the awarding bureaus a means of discipline that requires no prosecution at all.[153] The central government therefore holds both a criminal and a contractual instrument capable of reaching how its contractors operate, and applies the contractual one to how they bid. The amended Cybersecurity Law, in force since January 2026, raises the penalties available, expands personal liability for directly responsible individuals, and extends the law's reach to conduct abroad that endangers the PRC's cybersecurity rather than only to conduct harming critical infrastructure.[154] In the same period, the tools to correct how contractors operate were expanded, but correction still reached only how they bid. The commitment to use the legal framework is public. In 2026 the Minister of the MSS wrote that the Cybersecurity Law and the Counter-Espionage Law are to be implemented comprehensively.[155] The instruments exist, they have

150 Winnona DeSombre Bernsen (2025): Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace & Eugenio Benincasa (2026): Provincial Tasking, Cross-Provincial Execution: A Case-Based Look at How China Scales Cyber Operations

151 Ministry of Foreign Affairs of the PRC (2021): Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference on March 3, 2021 & Aj Vicens (2024): Chinese hackers are increasingly deploying ransomware, researchers say

152 Margin Research (2023): China's Cyber Laws and Regulations

153 Orange Cyberdefense (2026): The hidden network – How China unites state, corporate, and academic assets for cyber offensive campaigns & Natto Team (2023): i-SOON: Another Company in the APT41 Network

154 China Law Translate (2026): Cybersecurity Law of the People's Republic of China (2026 revised version) & The National People's Congress of the People's Republic of China (2025): Explanation of the Cybersecurity Law of the People's Republic of China (Draft Amendment) [translated by Claude Opus 5.5]

155 Chen Yixin (2026): Chen Yixin, Party Committee Secretary and Minister of the Ministry of State Security, publishes signed article in China Cyberspace magazine [translated by Claude Opus 5.5]

been strengthened, and the ministry that tasks the operators has said publicly that they will be applied.

At the technical layer, tradecraft has improved: incident responders report PRC-nexus actors building custom malware ecosystems, exploiting zero-day vulnerabilities in security appliances, operating through proxy networks, moving onto edge platforms that carry no endpoint detection, and obfuscating their malware to frustrate analysis – all of it aimed at evading detection and remaining resident longer.[156] Some of it, above all the move to covert networks built from compromised devices, makes attribution harder as well as detection.[157] Evading detection and evading attribution are different aims. Public sources do not settle how far rising attribution drove that move, or whether the state minds its military units being named more than its contractors. The move may respond to outside pressure, serve longer collection, or both.

What has not changed is the conduct that generates attribution in the first place. Contractors still initiate intrusions and sell them afterward, state tasking still runs alongside private crime, and public vulnerabilities are still exploited at scale within hours of disclosure. The investment has gone into hiding better, not into operating more carefully. A central government that routinely disciplines financial misconduct among its contractors while tolerating loud, attributable operations has not lost the ability to correct. **It corrects selectively, and selective correction is a sign that delegation still works.**[158]

Procurement discipline runs through military contracting organs and anti-corruption enforcement, however, while the tasking of intrusions runs through the security services and their bureaus. The security services' own procurement is far less visible, so whether they have disciplined their suppliers over how they operate cannot be observed directly. Had they acted on tradecraft, the effect would show in how contractors operate, and it does not. What the debarments establish is therefore narrower than it first appears. These firms are reachable by the state

156 Jurgen Kutscher (2025): M-Trends 2025: Data, Insights, and Recommendations From the Frontlines

157 Michael Raggi (2024): IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders

158 How far the center controls what happens below it is a long-standing question in China studies. One strand stresses the limits of central control in a fragmented bureaucracy. Another shows local agents carrying out what the center enforces as a priority and neglecting what it does not. Both fit the pattern described here: control that is real where the center prioritizes it, and loose where it does not. See Kenneth Lieberthal, Michel Oksenberg (1988): Policy Making in China: Leaders, Structures, and Processes & Kevin J. O'Brien and Lianjiang Li (1996): Selective Policy Implementation in Rural China & Andrew Mertha (2009): "Fragmented Authoritarianism 2.0": Political Pluralization in the Chinese Policy Process

and the state acts against them when their conduct affects its own interests. They do not establish that a specific instruction to tighten tradecraft was considered and refused. The narrower finding is sufficient, however. Contractors that can be suspended within months of a procurement irregularity are not beyond the state's reach.

The same selectivity appears in a second domain, and at a far greater scale. Cyber-enabled fraud run by Chinese criminal networks has drawn a sustained state response: four national enforcement campaigns between 2020 and 2024, a dedicated law on telecom and online fraud in force since December 2022, a nationwide network of provincial and municipal anti-fraud centers, and joint operations with neighboring states that led to tens of thousands of arrests of Chinese nationals abroad.[159] The state did not run the scam compounds, yet sustained pressure still pushed it to act against them. Most of that pressure came from inside China: from the harm done to Chinese citizens, and from the damage the compounds did to relations with neighboring states. Correction came once the state's own interests were at stake, the same threshold seen in the contracting cases.

The law reaches fraud committed by Chinese citizens outside the PRC and imposes direct obligations on banks, telecommunications operators, and platforms. A state that enforces at this scale has the means to discipline nationals who run cyber-enabled operations from abroad.

Here too, enforcement is uneven. Some operators whose networks serve wider state interests have remained unprosecuted at home while under sanction abroad, and enforcement is assessed to have concentrated on operations targeting Chinese victims, with the effect that criminal groups redirected toward foreign ones.[160] The institutions differ in part from those that task and buy cyber operations, and the comparison is limited accordingly. What it establishes is narrower and still useful: in the cyber domain, correction is available, it is applied at scale when the harm falls on the PRC's interests, and it is withheld where the actor is useful or the harm is borne elsewhere.

159 China Law Translate (2022): Law on Countering Telecommunications Network Fraud & Xinhua (2025): China, Myanmar, Thailand endeavour to eradicate telecom fraud networks & Junqing Zhang (2026): China's selective anti-scam campaign poses a paradox for Southeast Asia & Supreme People's Procuratorate of the People's Republic of China (2025): Prosecutors to intensify fight against telecom fraud & Eugenio Benincasa (2026): Cybercrime Pushed Fraud Offshore – and Ignited a U.S. Crackdown

160 U.S.-China Economic and Security Review Commission (2025): China's Exploitation of Scam Centers in Southeast Asia

Sustained bilateral pressure culminating in a 2015 agreement on commercial cyber espionage was followed by a measurable decline in Chinese operations against commercial targets in the United States, and, shortly before the agreement, by reported arrests of individuals identified by American authorities.[161] Here, correction reached how operators operate.

It did not hold. Activity resumed within a few years.[162] There are two explanations, and both can be true. The decline had begun in mid-2014, over a year ahead of the agreement, as military reforms centralized the PLA's cyber units and public exposure and US pressure took effect. Part of what was read as a reduction was therefore a reorganization already under way.[163] Economic espionage is assessed to have passed largely from PLA units to the MSS, whose own tradecraft was better than the PLA's, and to its contractors, whose tradecraft varies widely, as the leaks since 2024 show (3.1).[164] The other reading is that the pressure was not kept up (5.4).

The same pattern appeared earlier, outside the cyber domain. Whether Beijing cannot or will not control what firms on its territory do has been asked before – about missile and chemical exports in the 1990s, and about fentanyl precursors more recently. Each time, controls tightened when the issue reached the bilateral relationship. Comprehensive missile export-control regulations followed years of US sanctions on Chinese firms. Class-wide scheduling of fentanyl-related substances followed a leaders' agreement in December 2018. Cooperation on precursors was suspended in August 2022 after the US House Speaker visited Taiwan, and resumed after a summit in November 2023.[165] If the state can suspend and resume enforcement depending on the relationship, it controls that enforcement.

The threshold at which the central government corrects its operators' conduct does exist, but it sits at the level of damage to a major bilateral relationship and not at the level of routine attribution. And when that correction came, it

161 John W. Rollins (2015): U.S.-China Cyber Agreement

162 Chris Bing (2018): Trump administration says China broke Obama-Xi hacking agreement

163 FireEye iSIGHT Intelligence (2016): Red Line Drawn: China Recalculates Its Use of Cyber Espionage

164 Adam Kozy (2022): Testimony before the U.S.-China Economic and Security Review Commission Hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States"

165 Evan S. Medeiros (2007): Reluctant Restraint: The Evolution of China's Nonproliferation Policies and Practices, 1980–2004 & Shirley A. Kan (2012): China and Proliferation of Weapons of Mass Destruction and Missiles: Policy Issues & Congressional Research Service (2024): Illicit Fentanyl and China's Role & Vanda Felbab-Brown (2024): The fentanyl pipeline and China's role in the US opioid crisis

changed what was targeted – commercial espionage against US firms – more than how much activity there was overall or the tradecraft threat actors used.

3.3 Operational Ceiling

The upper boundary is the ceiling. Though extensive intelligence collection has been observed, alongside access collection to critical infrastructure, no PRC cyber campaign has to date been shown to aim at disrupting the operation of those systems.[166] Disruption has occurred where the aim is unclear. In November 2022, ransomware that researchers link to a suspected Chinese espionage group put India's leading public hospital onto manual operation for days. Delhi police said no ransom had been demanded, and why the group used ransomware has not been established.[167] Espionage groups have used ransomware to distract investigators, to point attribution elsewhere or to remove evidence, as well as to disrupt. PRC operators have gained access to power, water, and transportation systems in the United States and elsewhere but have not used it to disrupt them. Not all of that access was gathered with disruption in mind. Some of it comes from broad, opportunistic compromise, including by contractors looking for something to sell (3.1). The concern is the access held for years in operational networks, where it offers little intelligence value, and its non-use is no reassurance. Read against the PLA's documented pursuit of "system destruction warfare", access of this kind is harder to dismiss as collection alone.[168] A senior US official has characterized the relevant access as unambiguous – persistent access held for possible disruptive effect instead of intelligence collection – which, if accepted, leaves non-execution as the only thing still holding the ceiling in place.[169] That characterization is an interpretation of what the adversary intends, not something observable. Even on what can be observed, the ceiling limits only the use of access. Preparation continues.

---

166 Cybersecurity & Infrastructure Security Agency (2024): U.S. and International Partners Publish Cybersecurity Advisory on People's Republic of China State-Sponsored Hacking of U.S. Critical Infrastructure & Sven Herpig (2025): Assessing Irresponsibility in Cyber Operations – A Guide for Operators and Decision-Makers in Times of Strategic Competition & Trend Micro (2020): Targeted Ransomware Attack Hits Taiwan Organizations

167 Aleksandar Milenkoski and Julian-Ferdinand Vögele (2024): ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware & Ani (2022): India: Hacked AIIMS server out of order for 6th day, Delhi police say no ransom demand made

168 Jeffrey Engstrom (2018): Systems Confrontation and System Destruction Warfare – How the Chinese People's Liberation Army Seeks to Wage Modern Warfare

169 Cybersecurity & Infrastructure Security Agency (2024): Opening Statement by CISA Director Jen Easterly & Jen Easterley and Christopher Wray (2024): Testimonies on The CCP Cyber Threat to the American Homeland and National Security at the U.S. Select Committee on the Chinese Communist Party

Between 2020 and 2022, intrusions attributed to PRC state-sponsored actors reached at least ten Indian power sector organizations.[170] The analysts who tracked the activity drew the same conclusion from the data: targeting of this kind offers little economic espionage or conventional intelligence value, and the tooling used was the shared backdoor whose origins are traced to MSS contractors who later supplied it to others. Years of access to grid control systems at targets with little intelligence value are often read as prepositioning.

Two caveats apply. The first is that restraint is hard to tell apart from the absence of an occasion to act. It is also hard to tell apart from access that falls short of what disruption requires. **No contingency has arisen in which disrupting the operation of foreign critical infrastructure would have served a Chinese objective, so the ceiling has not been tested under the conditions that would matter most.** A smaller occasion did arise. In May 2020, access held for months inside Taiwan's state-owned petroleum company was executed against payment and business systems, while production was left untouched.[171] The access was used, but only up to a point. The case is also read as a signal. The firm that investigated it judged the aim to be political deterrence, citing the missing decryption instructions and the timing, a week before the president's second inauguration.[172] Both readings fit: a signal aimed at business systems could be sent, denied and absorbed without coming near the ceiling. The second caveat concerns what counts. Disrupting a company's payment systems is not the same as disrupting the infrastructure it operates, and the ceiling refers to the second, pursued as the aim of a campaign.

Both caveats point in the same direction. Taiwan is the clearest case in which collected access has been executed, and the one place where a contingency severe enough to test the ceiling is most likely to occur. The occasion need not be a war. Access already in place lets the PRC raise the pressure in a crisis below the level of conflict, in ways it could deny and later undo, and having that option may make using it more likely.[173] A ceiling held only by non-execution can be tested in a crisis well before it is tested in a war.

---

170 Insikt Group (2022): Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group

171 Unnamed (2020): Bureau names ransomware culprits & Sean Lyngaas (2020): Taiwan suggests China's Winnti group is behind ransomware attack on state oil company & Trend Micro (2020): Targeted Ransomware Attack Hits Taiwan Organizations

172 CyCraft (2021): China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware

173 Adam Segal and Matthew Ferren (2026): Changing China's Cyber Calculus

3.4 Countervailing Evidence

The reading offered here – bounded delegation, correction withheld, a ceiling that has held so far – is neater than the evidence. Three considerations cut against it.

The first is that the PRC's response to pressure cannot be predicted from the record, even though what it tolerates and avoids can. Where a response can be traced, it does not suggest a fragile system. Repeated court-authorized takedowns of operational infrastructure were followed not by retreat but by wider adoption of covert networks across the majority of PRC-nexus actors, with those networks rebuilt and, in the words of an allied advisory, kept "constantly updated".[174] Infrastructure of this kind is built to be abandoned and replaced, and its loss is a cost that capable state actors plan for.[175] Where the infrastructure belongs to a commercial supplier, the cost falls first on that supplier. A takedown removes the service it sells, it has to rebuild before it can sell again, and its customers can turn to competitors in the meantime (6.2). For the state that buys from this market, the cost is small and passes quickly, since other suppliers are ready to step in. Costs that are not routine have been absorbed as well. Contractors under foreign sanctions have continued to operate, and one of them kept its tools online after designations in three jurisdictions (5.4, 6.2). **The PRC's response to cost, where it can be traced, has been to absorb and not to change behavior.**

The second consideration matters most for the argument, because it places part of the disorder with the central government itself. Disorder does not necessarily originate at the edge. A central government that sets urgent tasking, rewards speed, and disperses execution across front companies and academic institutions generates pressures of its own, and those pressures can degrade control as readily as delegation does. Political pressure and urgency are assessed to contribute more to loss of control than delegation to contractors.[176] This is not unique to the Chinese decision-making ecosystem.

The central government therefore cannot set the level of looseness at will. A further possibility is that the disorder comes from the structure. Vendor analysis

174 Cybersecurity & Infrastructure Security Agency (2026): Defending Against China-Nexus Covert Networks of Compromised Devices & Tom Uren (2026): Srsly Risky Biz: US Vows to Fight Distillation Attacks

175 Michael Raggi (2024): IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders

176 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

of the contracting layer holds that the depth of Chinese subcontracting makes auditing and supervision by the central government and its agencies progressively harder, risking inconsistencies in operational security and raising the likelihood of errors that expose operations or their sponsors.[177]

The difficulty of supervising a deep subcontracting chain may explain how individual errors occur, but it does not explain why they persist. If a structure keeps producing such errors for a decade, in plain view, the state has accepted its output. Whether the state designed this looseness matters less than whether it accepts the rate of errors that results, as the price of what the system delivers. The PRC's behavior indicates that it does.

Lastly, there is the question of comparison. Other capable states also work through contractors, lose tools to proliferation, and rely on commercial suppliers.[178] Established scholarship on cyber proxies has mapped these relationships along a spectrum of state influence, distinguishing delegation from looser forms of enlistment and from mere permission, and has treated the degree and intensity of state support as what determines whether responsibility attaches.[179] Recent work asks the same accountability question about the Russian proxy ecosystem, and answers it with two measures that overlap with those set out here: disruption and cost imposition.[180] The PRC is therefore not alone in delegating, and delegation is not a new object of study.

Nonetheless, the PRC's activities show that its delegation is distinct in three important features. The first is the size of the delegated layer, which reaches across contractors, public universities, state-owned enterprises, and a militia reserve, and not only a portfolio of vetted firms.[181] The second is legal compulsion. In the PRC, reporting duties and cooperation obligations push privately discovered vulnerabilities toward the state. This has no equivalent in other states with a strong cybersecurity posture. The third is that exposure carries no internal cost, whereas comparable states such as the US have faced institutional consequences

177 Orange Cyberdefense (2026): The hidden network – How China unites state, corporate, and academic assets for cyber offensive campaigns

178 E. g. SentinelOne (2026): EternalBlue Exploit: What It Is And How It Works & Michael Barnhart (2025): Defense to Danger: An Insider's Sale of Cyber Weapons

179 Tim Maurer (2018): Cyber Mercenaries: The State, Hackers, and Power & Florian J. Egloff (2022): Semi-State Actors in Cybersecurity & Erica D. Borghard and Shawn W. Lonergan (2016): Can States Calculate the Risks of Using Cyber Proxies? & Jason Healey (2012): Beyond Attribution: Seeking National Responsibility for Cyber Attacks

180 Joyce Hakmeh, Harriet Moynihan, and Nayana Prakash (2026): Holding state-sponsored hackers and other cyber proxies to account

181 Huseyin Can Yuceel (2026): Chinese Threat Actors: What Defenders Need to Know

after major losses of their own tooling.[182] **While delegation is common state practice, delegation on this scale, fed by compulsion, and costing nothing when it goes wrong, is not.**

182 Oleksii Baranovskyi (2017): How did NotPetya cost businesses over $10 Billion in damages & Nicole Perlroth and Scott Shane (2019): In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc & Amy Zegart (2017): The NSA Confronts a Problem of Its Own Making & Dave Lee (2017): Global cyber-attack: How roots can be traced to the US & Unnamed (2019): Baltimore ransomware attack: NSA faces questions & Shannon Vavra (2019): Sen. Van Hollen: Government sees no EternalBlue in Baltimore ransomware attack

4. Record: Campaigns Examined

Six PRC-attributed cases are examined to assess where state responsibility attaches.[183] Each case is set out as it occurred and then run through the same three sets of questions, so that the judgment rests on a repeatable test:

1. What makes the case look like a loss of control?
2. What shows the looseness to have been tolerated instead of lost? Was correction available and withheld? Was tasking or purchasing continued despite the disorder?
3. Where does irresponsibility attach to the operation?

One limit applies to all six cases. Operations usually become public when something about them goes wrong – activity is detected, a tool is captured, a contractor is indicted, or a leak exposes a client list. Operations that run well stay out of view. The six cases therefore show what is tolerated at the visible end of the range.

4.1 AI Automation (GTG-1002)

A vendor investigation reported a PRC-attributed espionage campaign, tracked as GTG-1002, in which an AI agent orchestrated the intrusion chain rather than merely assisting with parts of it. According to that reporting, the operators broke the campaign into discrete sub-tasks, each of which looked legitimate when assessed on its own, and the agent then carried out some 80 to 90 percent of the tactical work by itself, at request rates no human team could match.[184] Separate reporting on the VoidLink framework describes an implant suite written almost entirely by an AI agent, with a first working build produced inside a week.[185]

At first sight, this is the case in the set where operators and the central government most clearly lack technical control. At the tactical layer, no human was in the loop. But two points matter. First, the autonomy was built in on purpose. Humans

183 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

184 Anthropic (2025): Disrupting the first reported AI-orchestrated cyber espionage campaign

185 Check Point Research (2026): VoidLink: Evidence That the Era of Advanced AI-Generated Malware Has Begun

remained at the points where tasks were set and decisions escalated, and the agent worked within the boundaries they drew. Second, the evidence is vendor-reported, and the claims are assessed to have come with limited tangible support.[186]

Using automation is not irresponsible per se. Neither is using AI for operational tempo. Deploying AI agents at machine speed without testing them or being able to stop them is.[187] Deploying self-propagating or agentic tools without close monitoring and kill switches is one of the most serious technical risks in this area.

A later operation, by the actor tracked as GTG-10007, takes the same model further. Between December 2025 and August 2026, a group assessed as operating from Hunan province ran parallel workstreams on shared tooling, with persistent campaign records that preserved context between sessions and with collection and vulnerability research that continued while the operators were absent. Thirteen AI agents were left running on a schedule to collect material, and roughly fifty organizations were targeted across education, energy, healthcare, finance, and multiple governments. A second workflow then sorted through what had been collected, judged what was worth reading, wrote it up like an intelligence report and put it somewhere the material could be picked up.[188] Two of the operators were identified as undergraduates at a university in Hunan, one of whom had interned at Sangfor, a Chinese technology and cybersecurity company, and was interviewing for an offensive cyber operations role at Qi An Xin, one of the large Chinese security firms that hold state contracts.[189]

Google's threat intelligence reporting shows the same shift beyond these two groups. It describes an unnamed PRC-nexus actor running the open agentic frameworks Hexstrike and Strix to scan targets and validate vulnerabilities with little human oversight. A second unnamed China-nexus actor turned to Gemini for help at nearly every stage, from reconnaissance and phishing through to lateral movement, command and control, and exfiltration. A third, APT41, used the same model to help write its tooling.[190]

186 Anthropic (2025): Disrupting the first reported AI-orchestrated cyber espionage campaign

187 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

188 Anthropic (2026): Detecting and countering misuse of AI: September 2026

189 Anthropic (2026): Detecting and countering misuse of AI: September 2026

190 Google Threat Intelligence Group (2026): GTIG AI Threat Tracker: Adversaries Leverage AI for Vulnerability Exploitation, Augmented Operations, and Initial Access & Google Threat Intelligence Group (2025): GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools

4.2 Untested Tooling (React2Shell)

On December 3, 2025, a maximum-severity vulnerability in React Server Components was disclosed, tracked as CVE-2025-55182 and named React2Shell.[191] Within hours of disclosure, threat intelligence teams observed exploitation attempts from PRC-nexus clusters, reported as including Earth Lamia and Jackpot Panda alongside clusters not attributed to any known group.[192] Tens of thousands of internet-facing instances were assessed as vulnerable.[193] Criminal actors exploited the same flaw in parallel for cryptomining and credential theft, and attribution was complicated throughout by the shared obfuscation infrastructure on which several unrelated operators depend.[194]

The tools the operators used matter as much as their speed. Around 145 proof-of-concept exploits circulated in the weeks after disclosure, of varying quality, and most did not trigger the underlying vulnerability. Assessments of the exploitation wave describe attackers prioritizing speed over precision, deploying flawed and incomplete public code across large parts of the internet, with many of those exploits resting on assumptions that do not hold in real deployments. Even so, the approach found some vulnerable systems. Some operators monitored new disclosures and folded public exploit code into their scanning infrastructure within hours. Others worked at it by hand, with one unattributed cluster spending close to an hour on a single target, adjusting its attempts as they failed.[195]

The case looks like loss of control chiefly in its target selection. At that tempo, the operators took what was reachable rather than what they had set out to find, and much of what they deployed did not work. Two points argue against that reading.

---

191 The React Team (2025): Critical Security Vulnerability in React Server Components & Eduard Kovacs (2025): Exploitation of React2Shell Surges

192 CJ Moses (2025): China-nexus cyber threat groups rapidly exploit React2Shell vulnerability (CVE-2025-55182) & Insikt Group (2025): Critical React2Shell Vulnerability Under Active Exploitation by Chinese Threat Actors & Justin Moore (2025): Exploitation of Critical Vulnerability in React Server Components (Updated December 12)

193 The Shadowserver Foundation (2026): Time series on cve-2025-55182

194 Shir Tamari, Gili Tikochinski, Hila Ramati, and Benjamin Read (2025): React2Shell: Technical Deep-Dive & In-the-Wild Exploitation of CVE-2025-55182 & CJ Moses (2025): China-nexus cyber threat groups rapidly exploit React2Shell vulnerability (CVE-2025-55182)

195 Peter Girnus, Deep Patel, Jack Walsh, Lucas Silva, and Ashish Verma (2025): CVE-2025-55182: React2Shell Analysis, Proof-of-Concept Chaos, and In-the-Wild Exploitation & CJ Moses (2025): China-nexus cyber threat groups rapidly exploit React2Shell vulnerability (CVE-2025-55182) & Cyble (2025): Zero-Day to Zero-Hour: React2Shell (CVE-2025-55182) Becomes One of the Most Rapidly Weaponized RSC Vulnerability & Aragorn Tseng, Robert Weiner, Casey Charrier, Zander Work, Genevieve Stark, and Austin Larsen (2025): Multiple Threat Actors Exploit React2Shell (CVE-2025-55182)

First, speed of this kind is a capability and not an accident. Turning a public disclosure into exploitation attempts within hours requires operators standing ready to act on published vulnerability research the moment it appears, and a system organized to use that research at scale. Second, the difficulty of attributing the activity is telling. **Where several operators work through infrastructure that a commercial supplier sells to more than one customer, and where the same public exploit code is used by state-linked groups and criminal actors alike, the activity can be traced to the ecosystem but not to any single unit. This is how a shared supply layer is expected to work, and the state leaves it that way.**[196]

Irresponsibility attaches at two points.[197] The first is the indiscriminate exploitation of a general-purpose framework, where the systems affected cannot be known in advance and include bystanders in every sector. The second is the use of untested and defective exploit code against live systems: deploying code whose behavior the operator has not established, at targets it has not selected, places the consequences beyond anything the operator can foresee or contain.

4.3 Shared Tooling (PlugX)

PlugX is a remote-access tool that has circulated among Chinese state-linked operators for well over a decade, shared instead of being held exclusively.[198] One self-propagating variant deployed by Mustang Panda spread by USB device across five continents, copying itself to any removable drive it encountered and therefore well beyond any target set an operator had chosen.[199] In September 2023, a French security company took ownership of the single command-and-control address the variant had been hard-coded to contact. Malware was removed from the infected machines in January 2025 by court-authorized action of United States and French authorities.[200] At no stage did the correction come from the Chinese government.

196 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

197 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

198 Sekoia (2026): What is PlugX malware? & malpedia (2026): PlugX

199 TDR Team and Félix Aime and Charles Meslay (2024): Unplugging PlugX: Sinkholing the PlugX USB worm botnet & Gabor Szappanos (2023): A border-hopping PlugX USB worm takes its act on the road

200 TDR Team and Félix Aime and Charles Meslay (2024): Unplugging PlugX: Sinkholing the PlugX USB worm botnet & Jessica Lyons (2025): FBI wipes Chinese PlugX malware from thousands of Windows PCs in America

In the same period, the same tool was used with considerably more care in a different PRC-attributed campaign. One cluster – tracked as TA416, overlapping with RedDelta and DarkPeony – ran target-selective campaigns against European governments and against diplomatic missions and delegations to NATO and the EU between mid-2025 and early 2026, timed to political events including the twenty-fifth EU–China summit.[201] It cycled through different delivery methods while keeping its custom payload updated. A campaign against Belgian and Hungarian diplomats, reported in October 2025, was attributed to the operator behind the self-propagating strain described above.[202]

A third cluster used freemail senders and far simpler infection chains to deliver the same tool against government, hospitality, and technology targets in South and Southeast Asia.[203]

The self-propagating strain is the strongest apparent case for loss of control among the six cases, and the one case where the reading of tolerated looseness does not hold cleanly. The strain had been publicly documented by security vendors for years beforehand, and no correction followed from the central government.[204] Evidence that the central government kept tasking or buying from the operator after the strain became public is weaker here than in the other cases. The closest the record comes is the operator's later campaigns against diplomats. The case therefore shows publicly documented looseness that went uncorrected, and only indirectly that it was accepted.

The wider lineage of PlugX uses, however, shows the same tool in very different hands. One cluster let it propagate untargeted across five continents, another used it with precision against diplomatic missions, timed to political events, and the operator behind the self-propagating strain has also run targeted campaigns against diplomats. A general lack of capability therefore does not explain what

---

201 Mark Kelly, Georgi Mladenov, and the Proofpoint Threat Research Team (2026): I'd come running back to EU again: TA416 resumes European government espionage campaigns & U.S. Department of Justice (2025): Justice Department and FBI Conduct International Operation to Delete Malware Used by China-Backed Hackers & Kevin Poireault (2026): Chinese Hackers Target European Governments in Espionage Campaigns

202 Mark Kelly, Georgi Mladenov, and the Proofpoint Threat Research Team (2026): I'd come running back to EU again: TA416 resumes European government espionage campaigns & Arctic Wolf Labs (2025): UNC6384 Weaponizes ZDI-CAN-25373 Vulnerability to Deploy PlugX Against Hungarian and Belgian Diplomatic Entities

203 Mark Kelly, Georgi Mladenov, and the Proofpoint Threat Research Team (2026): I'd come running back to EU again: TA416 resumes European government espionage campaigns & U.S. Department of Justice (2025): Justice Department and FBI Conduct International Operation to Delete Malware Used by China-Backed Hackers

204 Gabor Szappanos (2023): A border-hopping PlugX USB worm takes its act on the road & Mike Harbison and Jen Miller-Osborn (2023): Chinese PlugX Malware Hidden in Your USB Devices?

happened. The variance reflects choices about how carefully to operate. The tool is shared across the ecosystem with no standard of care attached, and the state lets the resulting differences in quality stand.[205]

Irresponsibility attaches at the release of self-propagating tooling and at the prolonged unmitigated access that follows.[206] The risk of reuse is not hypothetical here. The researchers who took ownership of the address noted that anyone able to do the same could send arbitrary commands to the infected machines and repurpose them for other ends.[207]

4.4 Exploit Proliferation (ProxyLogon)

In early 2021, a set of zero-day vulnerabilities in Microsoft Exchange Server was exploited in a targeted manner by a state-linked operator.[208] After the vendor released patches in March 2021, exploitation broadened sharply, with web shells left on tens of thousands of servers worldwide and access available to whoever found them, state and criminal alike. In one practitioner's account, the Chinese security services had kept the capability tightly held, but once the patch shipped it was "open season".[209] Related Exchange vulnerabilities were exploited later the same year. In July 2021, more than thirty states attributed the campaign jointly to China.[210]

Targeting on that scale, with access left standing for others to find, is the classic profile of an operation that has escaped its operators. The period before the patch, however, shows that control was possible. The same capability was handled narrowly for as long as narrow handling served a purpose. What

205 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

206 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

207 TDR Team and Félix Aime and Charles Meslay (2024): Unplugging PlugX: Sinkholing the PlugX USB worm botnet

208 Orange Tsai (2021): A New Attack Surface on MS Exchange Part 1 - ProxyLogon!

209 Shaun Waterman (2026): American Hackers-for-Hire Proposal Sparks Heavy Criticism

210 Council of the European Union (2021): China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory

changed at disclosure was the calculation, not the capability.[211] What followed has been read as a high political cost for little intelligence gain – a cost that was expected and accepted.

Irresponsibility attaches at the indiscriminate targeting and at access knowingly left in place for anyone to use.[212]

The same thing happened again in late August and September 2026, faster. An exploit kit named BlueMoon was first seen on August 28 in the hands of TA412, the MSS-linked actor also tracked as APT31 and tied to the Wuhan front company. Within six days three more espionage groups were using it, most of them China-aligned.[213] None of them was careful about it: the delivery domains were registered the same day the campaigns ran, and once the browser was exploited the kit simply fetched an executable from a remote server and ran it, far below the operational security normally seen with browser exploit chains.[214] Analysts offered possible explanations for how it spread so quickly: a shared commercial supplier selling to several state-aligned actors, or a central state body handing it out. In both cases, the capability was passed around, and in neither is the ecosystem operating out of the state's sight.[215]

211 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

212 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

213 Mark Kelly, Greg Lesnewich, Konstantin Klinger, Saher Naumaan, Julia Paluch, David Galazin, Stuart Del Caliz, and the Proofpoint Threat Research Team (2026): Once in a BlueMoon: Multiple State-Aligned Threat Actors Rapidly Adopt Novel Exploit Chain Using Chrome and Windows Zero-Days

214 Mark Kelly, Greg Lesnewich, Konstantin Klinger, Saher Naumaan, Julia Paluch, David Galazin, Stuart Del Caliz, and the Proofpoint Threat Research Team (2026): Once in a BlueMoon: Multiple State-Aligned Threat Actors Rapidly Adopt Novel Exploit Chain Using Chrome and Windows Zero-Days

215 Mark Kelly, Greg Lesnewich, Konstantin Klinger, Saher Naumaan, Julia Paluch, David Galazin, Stuart Del Caliz, and the Proofpoint Threat Research Team (2026): Once in a BlueMoon: Multiple State-Aligned Threat Actors Rapidly Adopt Novel Exploit Chain Using Chrome and Windows Zero-Days

4.5 Contractor Initiative (i-SOON)

A United States indictment unsealed in March 2025 documented the modus operandi of i-SOON. Some intrusions were conducted at the direct request of MSS and MPS bureaus. Others were conducted on the firm's own initiative, with access or stolen data offered for sale afterward.[216]

The second mode makes the case look like lost control: a private company selecting foreign targets on commercial judgment, without prior tasking by government entities. The counter-evidence is that this model was not hidden from the state customers who kept buying from it, across dozens of bureaus and several years.[217]

Correction, when it came, came from outside. The firm was indicted in the United States in March 2025 and placed under EU sanctions in March 2026, alongside two of its co-founders, for offensive services directed at the critical infrastructure of EU member states. No corresponding action against its conduct has been recorded in the PRC.[218] Correction was available in principle – firms in the same contractor market were disciplined by the PLA for collusive bidding in military procurement, although i-SOON's customers were security bureaus, whose discipline is rarely visible (3.2) – and where it was applied, it reached how contracts were won and not how intrusions were conducted.[219] In such cases the state is customer and enabler at once.

Irresponsibility attaches where the state keeps buying and therefore enables such self-initiated intrusions.[220] At that point, an affected state can assign part of the responsibility to the central government, without first having to prove the tasking chain.

---

216 U.S. Department of Justice (2025): Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns & Natto Thoughts (2026): i-SOON Leaks

217 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

218 Council of the European Union (2026): Council Decision (CFSP) 2026/588 of 16 March 2026 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

219 Eugenio Benincasa and Natto Team (2026): China's Cybersecurity Powerhouses Face PLA Procurement Curbs & Eduard Kovacs (2026): China's Top Cybersecurity Firms Hit by Mounting Military Procurement Bans

220 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

4.6 Mission Blending (APT41)

Chengdu 404 Network Technology presented itself as a network security firm while its staff conducted intrusions later charged in United States indictments in 2020.[221] The activity associated with APT41 combined state-directed espionage with financially motivated crime conducted for private gain. This included intrusions into the video-game sector and the use of access for revenue instead of intelligence.[222] Tooling used by this cluster, including the ShadowPad backdoor, circulated to other PRC-linked operators.[223]

An operator that runs state tasking and private profit-making through the same access is a case of weak organizational control. What matters is what happened after the exposure. Indictment and public identification did not lead the central government to end the arrangement. The company continued to operate, registered further software products and approached a municipal government body for financing support in the year that followed, and the shared tooling associated with the cluster stayed in circulation across other operators.[224] That is consistent with the finding that the PRC's contracting system imposes few costs on organizations whose operations are exposed or attributed.[225]

The irresponsibility lies in keeping espionage and crime blended over years.[226] Where the state lets access it supplied be used for private crime, a response should target the state that allows it, not only the individual operator.

221 U.S. Department of Justice (2020): Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally

222 Mandiant (2022): APT41, A Dual Espionage and Cyber Crime Operation

223 Daryna Olyniychuk (2023): ShadowPad Trojan Detection: Redfly Hackers Apply a Nefarious RAT to Hit National Power Grid Organization in Asia

224 Natto Team (2023): i-SOON: Another Company in the APT41 Network & Joey Chen, Ashley Shen, and Vitor Ventura (2024): APT41 likely compromised Taiwanese government-affiliated research institute with ShadowPad and Cobalt Strike

225 Winnona DeSombre Bernsen (2025): Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace

226 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

4.7 Case Findings

In four out of the six cases, what looks like lack or loss of control turns out to be looseness the central government could have corrected and did not. The remaining two resolve differently. In the PlugX case, the looseness was ended from the outside by foreign law-enforcement action. In the React2Shell case, there was no single point to correct, because unrelated operators used infrastructure that a commercial supplier sells to several customers. Neither case supports the lost-control reading, but neither is a clean case of tolerated looseness either. One thing holds across all six cases: none of them approaches the ceiling, a campaign aimed at disrupting the operation of critical infrastructure. None of the six shows the central government taking corrective action, so the cases say little about what would lead it to do so. Taken together, the cases place responsibility where the government built the conditions for the disorder and did not remove them, whether or not it directed the specific act.

5. Assessment: Normalized Statecraft

5.1 Delegation As Policy

Set against the record, the central government's control is high at the core and loose at the edge, where it tolerates contractors acting on their own initiative, espionage blended with crime, and tools that spread after use. Above both sits a ceiling: no PRC campaign has been shown to aim at disrupting the operation of foreign critical infrastructure such as power, water, or transport systems (3.3). The ceiling holds back the use of access. It does not hold back preparation, since access to such systems is still being gathered and held. The PRC's behavior in the cyber domain is best read as normalized statecraft: a routine foreign-policy instrument whose looseness is an accepted cost and not a sign of a state that has lost its grip. The assessment rests on observed behavior. It makes no claim about what the government may privately believe.[227]

For affected states, the implication is not reassuring. The looseness looks like lost control, but the state could correct it and does not. It tolerates more looseness than comparable states do in their own operations, and it pays no internal cost when operations go wrong (3.4). A system that the state has built up, that runs through others, and that has so far absorbed the costs imposed on it will not shrink on its own, and the concern it raises should not wait for a breach of the ceiling. **The Chinese government has not lost control of its cyber campaigns. It tolerates the looseness they produce, as the price of operating at scale. The delegation is the policy, and affected states are entitled to respond to it as such.**

5.2 State Responsibility

If not correcting creates responsibility, disorder in operations cannot be used to deny responsibility. **Instead of asking whether the state intended each act, ask whether it is responsible for what its system produces. That question can be answered without proving intent operation by operation.** This contests what

227 Assessment drawn from revealed behavior – outcomes tolerated versus avoided, read from the record and not from stated doctrine. "Normalized statecraft" is used here as a description of the observed pattern, not as an attribution of doctrine.

appears both in the PRC's doctrine and in the government's own defense – that activity conducted on private initiative dilutes state accountability, so that a contractor acting for its own reasons relieves the state of responsibility.[228] Where a state builds up a system, draws on it, and tolerates how it runs, the delegation is the policy. Private initiative does not absolve the central government of responsibility for having built and sustained the incentives and structure it takes place in. This assessment does not require proof of the tasking chain. Responsibility is shared, in unequal parts, between customer, tasker, executor, and enabler. Recent Chinese campaigns show this: firms have been named, but what each of them contributed has not been made public.[229]

The proxy literature classifies a relationship by the degree of state support and derives responsibility from that classification, which requires establishing what the state did for the actor. Where it allows for a state that merely tolerates a proxy, toleration is one category among several and is not used to assess a whole ecosystem.[230] The best-known version is a spectrum of state responsibility that runs from attacks a state prohibits, through attacks it ignores, encourages, shapes, coordinates or orders, to attacks it carries out itself.[231] The PRC record does not sit at one point on it. The same ecosystem contains operations run by state units, contractor work ordered by bureaus, contractor initiative the state buys from afterward, and criminal drift it leaves alone. The "out of control" reading places it where a state wants to stop activity but cannot, or where its own elements have gone rogue. The correction record rules out the first, since correction is available, and continued purchasing rules out the second. Bounded delegation describes that spread, and the lines the state draws within it. The approach taken here reads the same record for what the state declines to do – where correction is available and withheld – and derives responsibility from toleration and not from support. **This means that an operation no one instructed but no one corrected either sits inside the state's responsibility.** The Chinese case requires this reading, because state support varies widely across such a large system, while the pattern of non-correction stays the same.

The spectrum works for describing who did what. It does not answer what a state owes for the system in which the activity takes place. Assessing roles in

228 The White House (2015): Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference & Michael N. Schmitt (2017): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

229 Sveva Vittoria Scenarelli (2026): Understanding modern Chinese cyber operations means shifting from 'APT' to composite responsibility

230 Tim Maurer (2018): Cyber Mercenaries: The State, Hackers, and Power

231 Jason Healey (2012): Beyond Attribution: Seeking National Responsibility in Cyberspace

a campaign and assigning responsibility for the system behind it are separate questions. Where the state built the execution layer, declined to correct it, and kept buying its output, the absence of an instruction for a particular intrusion describes how the campaign was routed. It does not limit what the state answers for.[232]

Automation adds a further layer. A former senior US official has observed that operations running with less human direction give an aggressor a new kind of deniability: a state that cannot be sure an attack was directed, or even intended, may hesitate to retaliate.[233] The hesitation concerns the political response. Defenders still clean up a compromise in the same way, whoever is behind it. As automation grows, this argument will be made more often. It does not change what the state answers for. A government that builds an execution layer, equips it with tools that act with little supervision, and declines to correct what those tools do has not thereby narrowed its responsibility. It has widened the gap between what it instructs and what it produces.

Responding to the US disruption of Nanjing Xinjiuwei infrastructure, announced in August 2026, the Chinese embassy in Washington said the PRC firmly opposes and combats cyber operations in all their forms in accordance with the law, and urged the United States to stop using cybersecurity to discredit China.[234] The Chinese embassy in Prague had answered a Czech attribution fifteen months earlier in almost identical terms, adding that China does not encourage, support or condone such cyber activities.[235] Denials of this kind are what most states say when accused, and on their own they settle nothing.

Affected states can point out that Chinese law applies the same principle. Since 2015, Chinese criminal law has made it an offense to knowingly supply technical support, infrastructure or other help to online crime without committing it, so that liability reaches those who enable the offense as well as those who carry it out.[236]

232 Sveva Vittoria Scenarelli (2026): Understanding modern Chinese cyber operations means shifting from ‘APT’ to composite responsibility

233 Anne Neuberger (2026): The New Chinese Way of Cyberwar – How Beijing Will Weaponize Digital Chokepoints

234 Sean Lyngaas (2026): US says Chinese hackers hit hospitals, NASA, Senate and more

235 Embassy of the People’s Republic of China in the Czech Republic (2025): Spokesperson of the Chinese Embassy in the Czech Republic Answers Journalists’ Questions on Cybersecurity

236 China Law Translate (2015): People’s Republic of China Criminal Law Amendment (9)

5.3 System Trajectory

Based on the structure the PRC has built and maintained, three developments follow. First, a rising quantity of campaigns, as AI integration, commodity orchestration, and a competitive supplier market make operations cheaper and multiply who can run them.[237] Second, less concern about being named, as parity with the United States reduces the formerly weaker party's reason to avoid attribution.[238] Operators are still investing in staying undetected for longer if the operational goal requires it, and some of that investment makes attribution harder too (3.2), so the two trends will run side by side. Third, a widening gap in quality, with high-end campaigns at one pole and a tolerated stream of loose contractor operations at the other.[239]

The first development affects capabilities, not only speed. Chaining working exploits into a reliable browser attack has historically been rare, and costly enough that few actors could do it. The BlueMoon kit seen in September 2026 carried signs of AI-assisted development: long debugging notes, and a reference to a handover file of the kind used to pass work between model sessions. The exploits were likely built from Chromium's own published security fixes, which appear in public code before they reach shipping browsers.[240] Scarce exploits and scarce operators have been the two limits on what an offensive program can do, and both are easing at once. Beijing sees it the same way. In September 2026, the Minister of the MSS described cyber conflict as having entered a stage of industrialized vulnerabilities, fully automated attack and defense, and AI operating against AI, with some states and organizations now able to find vulnerabilities in bulk, chain attack paths automatically, and carry out complex intrusions – substantially lowering the technical threshold and the cost of conducting operations.[241] He was

237 Anthropic (2025): Disrupting the first reported AI-orchestrated cyber espionage campaign & Nathan Beauchamp-Mustafaga (2024): Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations – Chinese Military Strategies, Capabilities, and Intent

238 Alexander Martin (2026): China's cyber capabilities now equal to the US, warns Dutch intelligence & Jurgen Kutscher (2025): M-Trends 2025: Data, Insights, and Recommendations From the Frontlines

239 Derived from the case record set out in Chapter 4, where the disciplined pole appears in the AI Automation and access collection cases and the loose pole in Untested Tooling, Shared Tooling, and Exploit Proliferation.

240 Mark Kelly, Greg Lesnewich, Konstantin Klinger, Saher Naumaan, Julia Paluch, David Galazin, Stuart Del Caliz, and the Proofpoint Threat Research Team (2026): Once in a BlueMoon: Multiple State-Aligned Threat Actors Rapidly Adopt Novel Exploit Chain Using Chrome and Windows Zero-Days

241 Chen Yixin (2026): Chen Yixin, Party Committee Secretary and Minister of the Ministry of State Security, publishes signed article in China Cyberspace magazine [translated by Claude Opus 5.5]

describing a risk to China and not a capability China holds. The description of what the technology now makes possible is the same either way, and it comes from the ministry directly or indirectly responsible for a significant share of the cyber campaigns originating from the PRC.

The baseline against which this growth runs is already substantial: among publicly reported incidents, the PRC leads all other states in state-attributable cyber operations outside the Russian war against Ukraine.[242]

This trend can already be observed. Over four days in July 2026, a framework coordinating up to eight parallel AI agents mapped twenty-one connected government systems in Taiwan, compromised eighty-five employee accounts, extracted more than two thousand five hundred personnel records, and pivoted through single sign-on into internal systems before extending to the island's nuclear safety agency, government IT vendors and at least seven energy companies.[243] Taiwan's Digital Affairs Ministry assessed that the combination of techniques and the exploitation of secondary systems allowed the campaign to run faster, cheaper and at a considerably larger scale than conventional operations.[244] The same change is reaching the far end of the chain. The Zhengzhou contractor's client materials describe a system running domestic AI models to sort illegally obtained data, build timelines and generate reports, and its staff described the platform internally as delivering a leap in both the quality and the quantity of what they could supply.[245] Collection at scale has long been limited by how much anyone could read and analyze. That limit is easing as well.

The bar is also falling at the bottom of the market. In late September and early October 2026, an actor assessed as likely Chinese-speaking and financially motivated targeted South Korean financial institutions using ARTEX, an open-source tool that uses AI agents to run penetration tests, released in July by a

242 The European Repository of Cyber Incidents recorded 331 state or state-affiliated incidents between October 16, 2023 and October 15, 2026. Outside of armed conflict [manual selection for Russian war against the Ukraine], the PRC was the country of origin of 87 of those incidents, followed by Russia with 54. See European Repository of Cyber Incidents (2026): Detailed Table View.

243 Dream Research Labs (2026): Inside a Multi-Agent AI Framework Used to Compromise Government Entities in Asia & John Llu (2026): Hackers used autonomous AI agents to attack Taiwan. Is this the future of cyberwarfare?

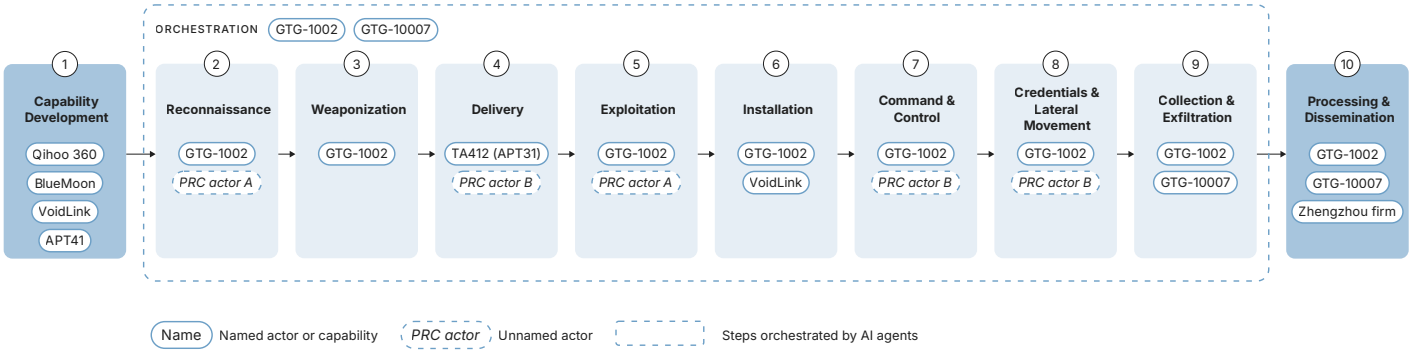
244 Ben Blanchard and Raphael Satter (2026): Taiwan says it was targeted last month in AI-driven hacking campaign

245 Josh Chin, Gabriele Steinhauser, and Tripti Lahiri (2026): How a Chinese Hacking Firm Tapped AI to Supercharge Cyber-Spying

Chinese developer, with a Chinese model as its main engine.[246] At least nine banks disclosed incidents or were reported as targets, and at one of them the personal data of around 25,000 customers was exposed.[247] The investigating vendor concluded that the tooling allowed one financially motivated actor to breach several organizations in quick succession.[248] That widens the circle of those able to run a campaign beyond the state's own operators and contractors.

How that case came to light matters as much as what it shows. Much of what is publicly known about AI use by PRC-nexus actors comes from Western model providers reporting misuse of their own models.[249] In the South Korean case the main model was Chinese, reached through a reseller, and the activity surfaced only because the actor left its session histories and configuration files on open servers.[250] The more operators use Chinese models, the less Western providers can see, and what stays visible is mostly the careless operators.

4 **PRC threat actor use of AI mapped against the intrusion chain**



Capability Development lists capabilities and those who built them; the other stages list the actors in AI-enabled operations at each step.
PRC actor A: unnamed suspected PRC-nexus actor using the agentic frameworks Hexstrike and Strix (Google Threat Intelligence Group, May 2026).
PRC actor B: unnamed suspected China-nexus actor using Gemini across intrusion stages (Google Threat Intelligence Group, November 2025).

Figure 4. PRC threat actor use of AI mapped against the intrusion chain.
View Figure 4 in full size (opens in a new window)

246 CrowdStrike Counter Adversary Operations (2026): Unknown Threat Actor Uses AI-Driven ARTEX to Target South Korean Finance

247 Kyu-seok Shim and Brenda Goh (2026): South Korean banks were likely hacked by a China-based actor with an AI agent, CrowdStrike says

248 CrowdStrike Counter Adversary Operations (2026): Unknown Threat Actor Uses AI-Driven ARTEX to Target South Korean Finance

249 Anthropic (2025): Disrupting the first reported AI-orchestrated cyber espionage campaign & Anthropic (2026): Detecting and countering misuse of AI: September 2026 & Google Threat Intelligence Group (2026): GTIG AI Threat Tracker: Adversaries Leverage AI for Vulnerability Exploitation, Augmented Operations, and Initial Access

250 CrowdStrike Counter Adversary Operations (2026): Unknown Threat Actor Uses AI-Driven ARTEX to Target South Korean Finance

5.4 Disincentive Gap

The returns from these campaigns are substantial. The costs imposed on the PRC in response have so far been small. This imbalance keeps the trend going. Affected states do not lack capability. The PRC collects political and military intelligence, advances the industrial priorities of its Five-Year Plans, collects access to critical infrastructure, and locates individuals abroad it treats as political threats. Against that, it has absorbed attributions, indictments, designations, and infrastructure takedowns without adjusting its conduct. The absorption is visible at the level of the firms as well as the government. Contractors placed on foreign sanctions lists have continued to operate inside China afterward, in some cases with continued state support. A listing cuts a firm off from foreign markets, banks, and jurisdictions, but does not touch its domestic business, which state contracts keep going.[251]

The problem confronting affected states is therefore a cost problem and not a capability problem. Affected states can work on both: the costs a campaign imposes on the state that runs it, and the returns it produces for the PRC. Affected states have pursued the costs more actively, with limited results. Three reasons explain why.

First, PRC activity has stayed below the threshold at which a decisive political response by affected states becomes likely. Effects are frequently invisible to the public, deniable in official exchanges, and individually insufficient to warrant action at the head-of-government level.

Second, responses by affected states have been scoped to incidents instead of to the pattern the incidents form. Attribution statements often describe the pattern: advisories set out years of activity, and the EU has recorded that PRC-linked activity against member states has increased in recent years.[252] The instruments themselves exist because of the overall volume of malicious activity, the EU's Cyber Diplomacy Toolbox[253] among them, but each use of them is tied to a single case. An indictment, sanction or takedown addresses a specific operation, firm or person,

251 Orange Cyberdefense (2026): The hidden network – How China unites state, corporate, and academic assets for cyber offensive campaigns

252 Cybersecurity & Infrastructure Security Agency (2024): PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure & Council of the European Union (2025): Cyber: Statement by the High Representative on behalf of the European Union on malicious behaviour in cyberspace against Czechia

253 European Union External Action (2026): Cybersecurity – What we do: Policies and actions

and the response ends there, while the campaign behind it often continues. Most activities never draw a response at all. As a result, the PRC has never been made to bear the cumulative weight of a decade of activity, and each response starts the count from zero instead of adding to it.

The 2025 Czech case shows this pattern. An EU member state completed a national attribution, the Union and NATO both issued statements of solidarity, and the affected foreign minister summoned the Chinese ambassador to warn of serious consequences for bilateral relations. But no consequence followed for the PRC. Attribution reached the coalition level, but cost imposition did not follow it there.

The Chinese response – a public rejection of the evidence and a complaint about the diplomatic handling – shows how costs are absorbed when the response stops at naming.[254] Cases outside Europe show the same ladder stopping at different heights. In January 2025, Japan's police agency and cybersecurity center jointly attributed more than two hundred incidents between 2019 and 2024 to a group they assessed as operating under PRC government direction, reaching the foreign and defense ministries, the space agency, politicians, journalists, and firms working on advanced technology. The response was an advisory calling on organizations to strengthen their defenses.[255] Six months later, Singapore disclosed that a threat actor was attacking its critical infrastructure, in what was described as the first public attribution of its kind by that state. The threat actor was named. However, the state behind it was not, and the responsible minister said the following day that naming the country was not in Singapore's interest at that point.[256] The signal still arrived: when local media linked the group to China, the Chinese embassy rejected "groundless smears and accusations against China".[257] Stopping short of naming the state is common in Southeast Asia, where governments that attribute at all tend to do

254 Council of the European Union (2025): Cyber: Statement by the High Representative on behalf of the European Union on malicious behaviour in cyberspace against Czechia & Karel Janicek and The Associated Press (2025): The U.S., EU, and NATO are rallying behind the Czech Republic, which says a hacking group associated with China's government attacked its critical infrastructure & North Atlantic Treaty Organization (2025): Statement of solidarity by the North Atlantic Council concerning the malicious cyber activities against the Czech Republic & Embassy of the People's Republic of China in the Czech Republic (2025): Spokesperson of the Chinese Embassy in the Czech Republic Answers Journalists' Questions on Cybersecurity

255 Alessandro Mascellino (2025): Japan Faces Prolonged Cyber-Attacks Linked to China's MirrorFace & Simon Sharwood (2025): Japanese police claim China ran five-year cyberattack campaign targeting local orgs

256 Louise Marie Hurel (2025): What Singapore's First Public Cyber Attribution Tells Us & FRANCE 24 (2025): Singapore facing 'serious' cyberattack by espionage group with alleged China ties

257 The Online Citizen (2025): China rebukes Singapore media over reports linking cyber group UNC3886 to Beijing & Tobias Feakin (2025): Calibrated Signals: How Middle Powers Are Rewriting the Rules of Cyber Attribution in the Indo-Pacific

so selectively and indirectly, in line with a broader reluctance to raise sensitive issues with China in public.[258]

Another case sits below both on the escalation ladder. In July 2025, a vendor reported a campaign against a government IT provider in an unnamed Southern African state, attributed with high confidence to a group long associated with Chinese interests and previously little seen in the region, seeking stored credentials, source code, and internal correspondence.[259] No government made a statement. The incident only became public because a commercial responder was present. The four cases descend an escalation ladder: attribution taken to the coalition level and answered with statements of solidarity (Czech Republic), attribution reaching the state and answered with an advisory (Japan), attribution deliberately stopping short of the state (Singapore), and no state response at all (Southern Africa).

The consequences applied to the state responsible have mainly been technical – infrastructure takedowns, seizures, advisories – and have not reached the economic and diplomatic channels to which the PRC has visibly reacted in the past. Measures taken to protect the systems attacked necessarily operate inside that domain. But reducing what a campaign yields is a separate question from raising what it costs. One former senior US official sums up the effect: **"We have trained them to believe the cost of intrusion is essentially zero".**[260] Serving officials make the same point. Announcing the August 2026 disruption, the serving US Attorney General said of the PRC conduct that "they know that we know that it's happening", and that they had raised it with Chinese counterparts for many years.[261]

Affected states do not lack instruments. Those used so far – technical disruption of operational infrastructure under judicial authority, criminal indictment of named operators, designation of firms and individuals under sanctions regimes, coordinated public attribution, and diplomatic representation – mostly reach

258 Gatra Priyandita (2025): Silence as strategy: Southeast Asia and China's persistent cyber campaigns

259 Kaspersky (2025): Kaspersky: APT41 targets Southern African organization in espionage attack

260 Rob Joyce (2026): China's Cyber Explosives are in Place. Where's our Response?

261 Sean Lyngaas (2026): US says Chinese hackers hit hospitals, NASA, Senate and more & Dan Mangan (2026): Politics & Policy Fed, NASA and DOJ among victims of Chinese state-sponsored hacker group: Court documents

operators and their suppliers, and they have been absorbed.[262] The instruments that reach the state – sanctions on state security and military entities, export controls, visa restrictions and other economic and diplomatic measures that affected states already use in other policy areas – have so far not been tied to cyber conduct (6.4). **Their use is constrained by the need for partners to act together and by economic dependence on the PRC. What is missing is the decision to use them for cyber conduct, and to keep using them.**

Others reach the same conclusion. A September 2026 assessment from the Council on Foreign Relations (CFR) finds that US disruptive actions against the PRC's cyber campaign ecosystem have produced real but limited results, and that they have been occasional and resource-intensive.[263] The same assessment notes that the PRC central government absorbs disruption, reconstitutes quickly, and has so far withstood the coercive campaigns directed at it. Both findings bear on what affected states should do. Occasional use can become routine through practice. The resource cost is a genuine limit, and it is a reason to concentrate disruption where one action reaches many operators (6.2), to stop rebuilding the evidentiary record for every case (6.6), and to carry more of the response through instruments that do not require a technical operation each time (6.4).

Two past responses suggest that costs can work when affected states apply them differently. The first is the sustained bilateral pressure that culminated in the 2015 agreement on commercial cyber espionage, which was followed by a measurable decline in operations against commercial targets.[264] But it had limits (3.2). What fell was the number of noisy, often PLA-run intrusions against US companies. What continued moved to more advanced MSS operators and their contractors, to targets outside the United States, many of them in Southeast Asia, and to targets such as defense contractors that the agreement arguably did not cover, since it

---

262 Recent analysis (Matthew Ferren (2026): The Trump Administration's Cyber Strategy Fundamentally Misunderstands China's Threat & Matthew Ferren (2026): Trump's Cyber Strategy Falls Short on China, Iran, and the Threats That Matter Most) makes a related argument from the other direction. Cyber operations serve four of the government's core interests: intelligence, technological self-sufficiency, political control, and prepositioning for a crisis. A response built around retaliation touches none of them, so treating offensive operations as the main answer misreads what the PRC is after. That critique starts from what Beijing gains. The reading here starts from what Beijing is willing to put up with. Both lead away from responses aimed at single operations, and toward responses aimed at the arrangement behind them. Whether affected states should run offensive operations of their own is a separate question, and it is not taken up here.

263 Matthew Ferren, Adam Segal, and Rush Doshi (2026): The Cyber Gap – How to Counter China's Threat to America's Critical Networks

264 John W. Rollins (2015): U.S.-China Cyber Agreement & Chris Bing (2018): Trump administration says China broke Obama-Xi hacking agreement

addressed espionage for commercial advantage.[265] Whether Beijing meant from the start to keep spying while avoiding detection, or changed course later as trade tensions rose, cannot be settled. The authors who documented the return set out both explanations.[266] For a future agreement, the lesson is the same either way: commitments need a clear scope, and compliance has to be judged by who is operating and against whom, as well as by how much activity one country sees.

Correction by the central government reached operational conduct on that one occasion, and it did so when the costs were applied visibly, across more than one domain, and at a level that engaged the bilateral relationship as a whole. There is a second explanation for why the effect did not last, and it lies with the United States. Two of the authors of that CFR assessment have since argued that cyber stayed at the top of the US–China agenda only from 2013 to 2015. Attributions, indictments and sanctions continued afterward at working level, but the attention of successive administrations shifted to trade, technology and military disputes, and Beijing concluded that Washington would protest and do little.[267] The second response is the joint attribution of the Microsoft Exchange campaign in July 2021, when more than thirty states attributed political responsibility to the PRC together – a degree of coordination not achieved before or, in the cyber domain, since.[268] It showed that states can name the PRC together. It did not show that pressure follows, because no lasting consequences came with it. Joint sanctions have been imposed as well. The United States and the United Kingdom imposed coordinated sanctions on the same APT31 front company and two of its staff in March 2024, and three jurisdictions listed Integrity Technology within fourteen months (6.2).[269] What has been missing is their use at scale and over time.

Among practitioners and researchers, what should follow from this is contested. Positions in the underlying research on how affected states should respond ranged across escalation, deliberate escalation intended to produce de-escalation, public naming and shaming, economic and political incentives, and the restriction of

265 Adam Segal and Lorand Laskai (2018): A New Old Threat – Countering the Return of Chinese Industrial Cyber Espionage

266 Adam Segal and Lorand Laskai (2018): A New Old Threat – Countering the Return of Chinese Industrial Cyber Espionage

267 Adam Segal and Matthew Ferren (2026): Changing China's Cyber Calculus

268 Council of the European Union (2021): China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory & Rob Joyce (2026): China's Cyber Explosives are in Place. Where's our Response?

269 U.S. Department of the Treasury (2024): Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure

access to advanced tooling.[270] No consensus emerged on which of these should carry the weight of a response. They did agree on two points: fragmented responses to single incidents play into the PRC's hands, and any effective answer has to build up over time and be coordinated.[271]

270 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

271 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

6. Response: Measures Available

The Athenians in Thucydides tell the Melians that **"the strong do what they can and the weak suffer what they must"**.[272] The line describes the relationship as most states affected by Chinese cyber campaigns appear to see it, and act on it. Part of the asymmetry comes from the kind of state the PRC is. It can compel firms, researchers and universities to serve its operations, and so sustain an ecosystem large enough to go after a wide range of targets at once (3.4). Democracies do not build ecosystems of this kind and could not compel one, and their responses have stayed modest for the reasons set out in 5.4. Chinese cyber campaigns proceed because they can, and affected states suffer the impact because, acting alone, they must.

That asymmetry comes from acting alone more than from a lack of capability. Individually, each affected state largely accepts what is done to it, including the United States. Collectively, they need not. Whether the Melian logic applies is therefore partly up to affected states, and the measures below are how they can change it. The most important is to hold the PRC responsible by default for any campaign with a China nexus. The others help apply that default. Disruption and attribution supply the evidence it rests on, collective cost imposition gives it force, and planning for a breach of the ceiling covers what has not happened yet.

The conduct of the PRC set out so far has a recognizable shape, and an effective response has to fit it. A single, centrally run adversary is the wrong model. The tools are the ones available against any state that works through proxies. What is specific is where they need to be aimed: at an execution layer of unusual size, held together by legal compulsion and a commercial market (3.4), and at a government that has corrected its operators only when the cost reached the relationship with other countries as a whole (3.2). PRC threat actor behavior covers a wide range, from disciplined operations to opportunistic contractor work, and the line between them is not neat. Across that range, campaigns tend to compromise broadly and to reuse shared access and tooling. Access held in critical infrastructures and elsewhere is meant to stay quiet, though it does not always, and collection runs from patient harvesting to smash-and-grab. No single instrument addresses all of that. An effective response has to work on several fronts at once: denying threat actors time inside networks and the returns they seek, degrading the shared supply layer, linking responsibility back to the state, and raising what the system costs the state that sustains it.

272 Thucydides (431 BC): The History of the Peloponnesian War

Repeated cost imposition at the infrastructure layer, for example by foreign law enforcement agencies, has so far been absorbed by PRC threat actors and not answered with restraint, likely because it is simply part of the cost of doing business for many of them. A domestic Chinese precedent points the same way. Sustained enforcement against cyber-enabled fraud networks – successive national campaigns, a dedicated law, and joint operations abroad – produced displacement instead of dismantlement. Networks relocated and reconstituted, arrests reached lower-level operators while the financiers behind the compounds escaped consequences, and the model has since expanded into new regions.[273] The comparison is inexact, since that enforcement was conducted by a state against its own nationals and with full domestic jurisdiction, while disruption by affected states operates without either. If enforcement with full jurisdiction only displaced these networks, disruption from abroad, without jurisdiction, cannot be expected to do more. Assessments of the Nanjing Xinjiuwei Network Technology Company infrastructure disruption reach the same conclusion. Action of that kind is described by a practitioner as "necessary to disrupting China's operations at scale [while] the robust market for offensive services in China guarantees their return to operations".[274] Individual disruptions work, but the Chinese ecosystem quickly rebuilds what was lost.

Disruptions of this kind weaken PRC infrastructure and produce evidence of who built, ran and used it. They do not dissolve it. The measures below are therefore presented as actions with observable effects. None of them is a reliable deterrent. Three of them build on each other. Disrupting the shared supply layer degrades capacity and produces an evidentiary record. That record supports attribution at the level of firms, universities, individuals, and the bureaus that task them. **Attribution at that level supports assigning responsibility to the state as a default rather than as a claim to be proven.**

The remaining four sit outside that sequence and do what it cannot. Collective cost imposition uses the evidence from all three steps at the level where correction has been seen once: the relationship as a whole, as before the 2015 agreement on commercial cyber espionage. Record consolidation[275] is the condition on which that application depends, and on which attribution, default responsibility, and any response agreed before a ceiling breach depend as well.

---

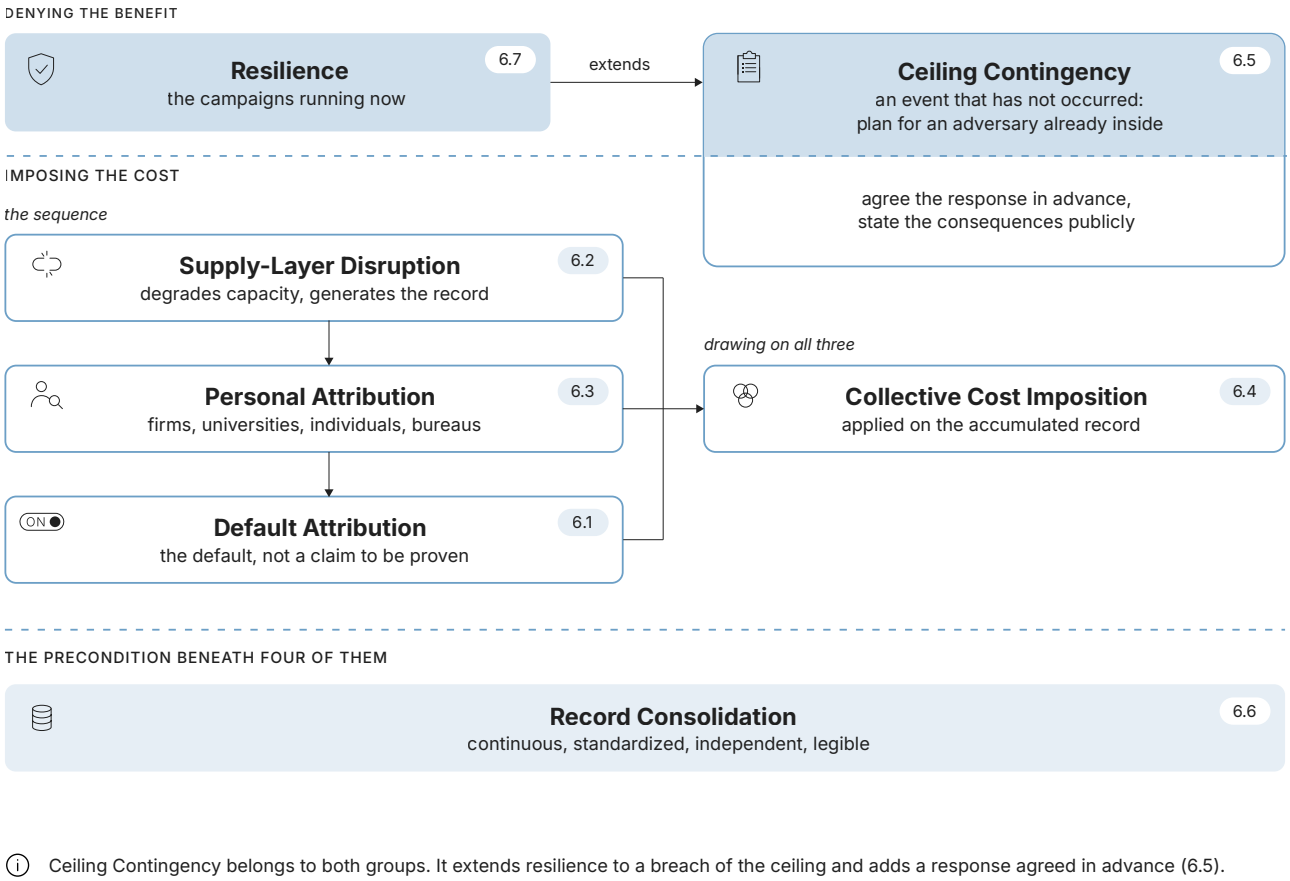
273 Eugenio Benincasa (2026): Whack-a-Mole: How China's War on Cybercrime Pushed Fraud Offshore – and Ignited a U.S. Crackdown & Jason G Tower (2026): China-linked scam operations pivot to Africa, presenting new challenges for at-risk countries

274 Sean Lyngaas (2026): US says Chinese hackers hit hospitals, NASA, Senate and more

275 Record consolidation means bringing the evidence that affected states already produce – from court-authorized disruptions, indictments, sanctions designations, joint advisories and technical reporting – into one continuous, shared record of PRC cyber campaigns, built to a published standard, so that responses can rest on the pattern of a decade of conduct (6.6).

Resilience and ceiling contingency sit next to each other, and the difference matters. The ceiling is the limit observed so far: no PRC campaign has been shown to aim at disrupting the operation of foreign critical infrastructure such as power, water or transport (3.3). It describes what has been observed. It guarantees nothing, and it has never been tested. Ceiling contingency means preparing for the day it is crossed. Resilience works on the campaigns running now: it reduces what an intrusion yields once it has succeeded, and it pays off whether or not any cost is imposed on the state behind it. Ceiling contingency applies resilience to a case that continuity planning does not usually cover – an adversary already inside the system, choosing the moment, and able to reach the systems used for recovery as easily as the main ones. It also adds two things resilience cannot: a coalition response agreed before the ceiling is crossed, and a public statement that holding persistent access in such systems will draw consequences.

5 Response measures available to affected states



ⓘ Ceiling Contingency belongs to both groups. It extends resilience to a breach of the ceiling and adds a response agreed in advance (6.5).

Figure 5. Response measures available to affected states.

6.1 Default Attribution

The opportunism and proliferation set out earlier are not evidence that the government has lost control. They are the tolerated by-product of a distributed model the central government built, declined to tighten, and continued to buy from. This has a direct consequence for affected states. The spreading of execution across contractors, universities, and front companies should not be allowed to reduce the responsibility borne by the state. **Where a campaign has a China nexus, the appropriate default is to hold the PRC accountable however indirectly the particular operation was tasked.** A China nexus here means that the operators, the firm employing them, the tasking or the infrastructure sit in the PRC. Where the activity is purely criminal, the state's share is its obligation not to let its territory be used for it, set out below. The default should not mean that every actor within bears the same responsibility. Responsibility remains composite, with operators, enablers, and the state carrying different and unequal shares for distinct parts of a campaign.[276] The narrower and firmer claim is that the state's share does not shrink because it chose to route execution through nominally private hands. Adopting that default across a coalition – in the language of attribution, in sanctions designations, and in diplomatic instruments – closes the escape route that bounded delegation gives the PRC. In practice, the default changes three things. Attribution statements name the state along with the firm, as the joint attribution of July 2021 began to do when it said the PRC had "fostered an intelligence enterprise that includes contract hackers".[277] Sanctions designations reach the bureaus that task contractors and the state entities that buy from them, as well as the contractors themselves. Diplomatic representations hold Beijing to account for a contractor's conduct without first having to prove that it ordered the intrusion. Governments may hesitate to say this openly. It invites the same charge against their own use of contractors, and it raises the political stakes of every attribution. Both risks are smaller when the default is stated jointly and in terms of norms all sides have endorsed, including the PRC (6.4).

The record set out here points to a state that has not lost control, and the framework of responsible state behavior that the PRC has itself negotiated and endorsed covers that case directly: states must not use proxies to commit

276 Sveva Vittoria Scenarelli (2026): Understanding modern Chinese cyber operations means shifting from 'APT' to composite responsibility & United Nations (2005): Responsibility of States for Internationally Wrongful Acts

277 The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China

internationally wrongful acts using information and communications technologies.[278] The recommendation also holds if that finding is wrong. A state that had lost control of contractors operating from its territory would still be expected not to knowingly allow its territory to be used for such acts, and to act against those committing them.[279] The PRC's own criminal law already makes unauthorized intrusion an offense, including when its nationals commit it abroad.[280] Both norms apply to internationally wrongful acts: conduct that is attributable to a state and breaches one of its international obligations.[281] That is clearest for operations that disrupt or damage. Whether espionage alone qualifies is contested. The case for holding the PRC responsible is therefore political as well as legal, and it does not depend on settling that question.

Either the PRC controls the execution layer, in which case the norms it has endorsed apply to what that layer does, or it does not, in which case its obligation is to bring it under control. There is no third position in which the campaigns belong to nobody. So far, the delegation model has worked as if there were. Default attribution closes that gap, and affected states can adopt it whichever reading of the evidence they accept. How much the choice of default matters is visible in a recent US instrument. A presidential memorandum of August 2026 allows vetted US companies to conduct surveillance and disruption operations against foreign cyber-enabled criminal groups. It covers only groups that are not "an institutional part of a foreign government or wholly operated under a foreign government's direction", and it treats a group as non-state unless there is clear intelligence of a link.[282] Bounded delegation falls between exactly these two options. On the record set out here, much of the PRC's contractor layer is neither part of the state nor wholly directed by it, and under the memorandum's presumption it would be treated as criminal. For disruption, that presumption widens what can be reached, and commentators have read it as aimed in part at state proxies.[283] Carried over into attribution, the same presumption would open the third position that the norms close: campaigns run by nominally private actors that no state answers for. Who may be disrupted

278 United Nations (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

279 United Nations (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security & International cyber law: interactive toolkit contributors (2025): National position of the People's Republic of China (2021)

280 Margin Research (2023): China's Cyber Laws and Regulations

281 International Law Commission (2001): Draft Articles on Responsibility of States for Internationally Wrongful Acts

282 The White House (2026): Expanding Capabilities to Combat Transnational Cyber-Enabled Crime

283 Aaron R. Cooper and Philip Chertoff (2026): White House Unveils Program to Authorize Private-Sector Cyber Surveillance and Disruption Operations

and who is responsible are separate questions. The answer to the first should not decide the second.

6.2 Supply-Layer Disruption

The inputs to Chinese cyber operations – initial access, covert infrastructure, and tooling – are not only owned by the units that use them but often also bought and sold. A covert network built by a commercial supplier may therefore serve several unrelated operators and bureaus at the same time. This is a weak point of the system and the most direct lever available to affected states, which is why they already use it. US authorities read the system the same way: contractors and other enablers are how the PRC extends its reach, so exposing and disrupting them narrows what the PRC can reach.[284] The disruptions of Raptor Train, the KV botnet, the residential proxy service known as 911 S5, and four distributed-denial-of-service botnets each removed capacity that several actors were drawing on at once.[285] The August 2026 seizures of Nanjing Xinjiuwei Network Technology Company infrastructure illustrate why the shared layer is the efficient target. The domains taken were hard-coded into both the scanning and the obfuscation tool for communication and authentication, so that removing them rendered both inoperable at once.[286] What makes the tools convenient for operators also makes them easy to take down together. Disrupting a shared layer reaches several operators at once, and that is the only kind of pressure that scales against operations that spread this widely.

The limit is that such networks are plentiful and interchangeable. They combine compromised devices with rented servers and purchased proxy services, and a network that is taken down is replaced from both (3.4). The rented part can be narrowed at the source, by requiring hosting and cloud providers to verify who their customers are. The United States proposed such a requirement for foreign

284 U.S. Department of Justice (2026): Justice Department and FBI Seize Vulnerability Scanning and Spear Phishing Tools Operated and Used by China-State Sponsored Hackers

285 U.S. Department of Justice (2024): Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers & U.S. Department of Justice (2024): U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure & U.S. Department of Justice (2024): 911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation

286 U.S. Department of Justice (2026): Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure & United States Attorney's Office (2026): Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure

customers in 2024 and withdrew it in December 2025.[287] At EU level, the NIS2 Directive requires verified registration data for domain names, but not for the rental of servers.[288]

Another advantage is that disruption is not confined to one legal model. The disruptions highlighted proceeded under United States judicial authorization.[289] Australia describes its own approach differently, stating publicly that its signals intelligence agency uses its own legal authorities for offensive operations that disrupt attackers' infrastructures, and that it acts with partners on server seizures and sanctions to raise the cost.[290] A third route runs through civil courts. In December 2021, Microsoft obtained a US federal court order to take control of 42 websites used by a PRC-linked group to spy on human rights groups, think tanks and government agencies in 29 countries. The company said at the time that the action would not stop the group's other operations.[291] The choice of legal basis is a national question. The availability of the measure, either via explicit case-by-case authorization or institutional mandates, is not.[292]

What followed these disruptions was wider use of covert networks across the majority of PRC-nexus actors, with those networks rebuilt and kept continuously updated.[293] Disruption should therefore be pursued for what it does achieve, including a direct cost to the supplier whose infrastructure is taken. It degrades capacity, raises the cost of rebuilding, and generates an evidentiary record under judicial authority. The remaining measures depend on that record.

The Raptor Train case shows how this works in practice. The botnet disrupted under the name Raptor Train was built and controlled by Integrity Technology

287 U.S. Department of Commerce (2024): Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities & Office of Information and Regulatory Affairs (2026): 2026 Unified Agenda of Regulations

288 European Union (2022): Directive (EU) 2022/2555 (NIS2 Directive)

289 The White House (2026): Expanding Capabilities to Combat Transnational Cyber-Enabled Crime

290 Australian Signals Directorate (2025): Annual Cyber Threat Report 2024-2025

291 Carly Page (2021): Microsoft seizes control of websites used by China-backed hackers & Netaskari (2026): Guest article: The Future-Past of digital espionage – APT15

292 See also Sven Herpig (2021): Active Cyber Defense Operations – Assessment and Safeguards & specifically for Germany Sven Herpig (2026): Stellungnahme von Dr. Sven Herpig, Lead Cybersecurity & Emerging Threats bei interface – Tech analysis and policy ideas for Europe e.V. (ehemals: Stiftung Neue Verantwortung), im Rahmen der Beteiligung von Spitzenverbänden, Fachkreisen und Verbänden zum Referentenentwurf des Bundesministeriums des Innern (BMI) für ein "Gesetz zur Stärkung der Cybersicherheit"

293 National Cyber Security Centre (2026): International cyber agencies share fresh advice to defend against China-linked covert networks

Group, a Beijing company that sold its customers access to infected devices through a commercial interface. A court-authorized operation in September 2024 took more than 200,000 devices out of the group's control and placed the company's role in PRC cyber campaigns on the public record.[294] A US designation followed in January 2025, and a British one in December 2025.[295] In March 2026, the European Union listed the same company, citing more than 65,000 devices compromised across six member states between 2022 and 2023, under the framework for restrictive measures established in 2019.[296] The disruption produced public evidence of the company's role, and that evidence made the later sanctions possible. The company could replace the botnet, but not do anything about the evidence against it. Eighteen months separated the first step from the last. The sequence did not end there. The company renewed the domains for its phishing tool in February 2026, a year after the US designation, and its scanning tool was still online in September 2026, six months after the EU listing. In October 2026, US authorities seized both, the second disruption of the same company in two years. The court filings state that "Integrity Tech has contracts with the PRC government".[297] Two disruptions and sanctions in three jurisdictions have produced a detailed public record of one contractor, and nothing in that record shows the PRC ceasing to buy from it.

Because the supply layer is commercial, it leaves records. A security researcher who spent months investigating the Nanjing Xinjiuwei Network Technology Company case put it simply: "If you're getting paying customers, you have a paper trail".[298] The same service that helped the operators hide may therefore have left a trail to them. **Concealment bought on a market comes with invoices, and invoices are evidence that technical indicators alone do not provide.**

294 U.S. Department of Justice (2024): Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers

295 U.S. Department of the Treasury (2025): Treasury Sanctions Technology Company for Support to Malicious Cyber Group & Alexander Martin (2025): British government sanctions Russian and Chinese groups over information warfare

296 Council of the European Union (2026): Cyber-attacks against the EU and its member states: Council sanctions three entities and two individuals

297 U.S. Department of Justice (2026): Justice Department and FBI Seize Vulnerability Scanning and Spear Phishing Tools Operated and Used by China-State Sponsored Hackers & U.S. Department of Justice (2026): Affidavit in Support of Application for Seizure Warrant, Western District of Pennsylvania

298 Sean Lyngaas (2026): US says Chinese hackers hit hospitals, NASA, Senate and more

6.3 Personal Attribution

Because the state relies on contractors, any single exposure can be dismissed as the act of a rogue firm. The answer is to name those behind the activity. That means naming not only the intrusion set, but the front companies or universities behind it, the individuals who staff them, and the provincial security bureaus that task them. Attribution of this kind from open sources has repeatedly come before formal charges, identifying front companies and named operators behind several major intrusion sets in advance of any indictment.[299] The practice is older than the current wave. In February 2013, a vendor report tied the group known as APT1 to PLA Unit 61398 and described individual operators by their online personas.[300] In May 2014, the United States indicted five officers of that unit.[301] Both were part of the pressure that preceded the 2015 agreement (3.2). The supply layer also makes defenders' analysis harder. Where several unrelated operators run through the same commercial infrastructure and the same purchased tooling, the groupings that defenders build from shared indicators no longer correspond to organizations, and activity that belongs to different customers of the same supplier is drawn together while activity belonging to one customer is split apart. Analysts of the Nanjing Xinjiuwei Network Technology Company case made the point plainly: the proliferation of firms offering niche offensive services makes Chinese operators more effective and makes it harder for defenders to cluster their activity.[302] Naming the supplier puts that activity back together, which is a reason to attribute at that level even if no legal consequence follows.

APT15, one of the longest-tracked PRC-linked groups, shows the cost of naming only the intrusion set. Activity grouped as APT15 dates back to at least 2010. Reporting has tied it to operations against European foreign ministries ahead of the 2013 G20 summit, against a company serving UK government departments in 2016 and 2017, and against Uyghur and Tibetan communities through surveillance apps.[303] Vendors still disagree on where the group begins and ends, and parallel

299 Kim Zetter (2022): Unmasking China's State Hackers

300 Mandiant (2013): APT1: Exposing One of China's Cyber Espionage Units

301 U.S. Department of Justice (2014): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage

302 Raphael Satter and AJ Vicens (2026): US Says Chinese Hackers Broke Into Justice Department, NASA, Federal Reserve, Senate & Sean Lyngaas (2026): US says Chinese hackers hit hospitals, NASA, Senate and more

303 FireEye (2013): FireEye Uncovers Chinese Cyber Espionage Campaign Targeting European Ministries of Foreign Affairs & Eduard Kovacs (2018): China-Linked Spies Used New Malware in U.K. Government Attack & Lookout (2024): BadBazaar: iOS and Android Surveillanceware by China's APT15 Used to Target Tibetans and Uyghurs

campaigns against the same communities are confused with it. Unlike the groups that US indictments have tied to individual MSS bureaus, it has no published indictment naming an operator.[304] The nearest the public record comes to an organization is indirect. An unsecured control panel of a surveillance app linked to the group only through shared servers exposed location data from test devices. The points clustered in one part of Xi'an, and one fell at the location of a defense contractor.[305] More than a decade of reporting has described what the group does and left the organization behind it unnamed.

Two refinements increase the pressure on those who take part in the PRC's cyber campaigns. First, the frictions within the market can be used against it. A contractor ecosystem driven by profit, moonlighting – official work during the day and crime, sometimes using the same tools, at night – and documented collusion over government contracts is one in which operators have reputations, rivalries, and finances that can be brought into the open. Corruption in such an ecosystem can be used to hold people to account. Second, sustained naming raises the personal cost of taking part and can put a front company out of use altogether. However, the effect is uneven. Some exposed groups have gone quiet: APT3 dropped out of sight in mid-2017, shortly after it was publicly tied to the firm Boyusec, although someone kept using its tools into 2018.[306] Others paused and then carried on: APT1 and APT12, both exposed in early 2013, moved to new infrastructure and were back at their earlier level of activity within about five months.[307] Naming individuals and firms therefore adds friction and links activity back to the state, but it is not a decisive blow.

Here too there is precedent. The same March 2026 listings by the EU named two individuals, co-founders of a sanctioned contractor, as responsible for cyber operations affecting member states – attribution at the level of the person and not the intrusion set, carrying an asset freeze and a travel ban.[308]

304 Netaskari (2026): Guest article: The Future-Past of digital espionage – APT15

305 Lookout (2024): BadBazaar: iOS and Android Surveillanceware by China's APT15 Used to Target Tibetans and Uyghurs

306 Symantec (2019): Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak & Kerstin Zettl-Schabath, Benjamin Butz and Camille Borrett (2023): Advanced Persistent Threat Profile – APT3/Boyusec

307 Phil Muncaster (2014): One year on: diplomatic fail as Chinese APT gangs get back to work

308 Council of the European Union (2026): COUNCIL DECISION (CFSP) 2026/588 of 16 March 2026 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

6.4 Collective Cost Imposition

The three measures set out above operate at the technical, legal, and declaratory levels. The one documented instance in which the central government corrected the operational conduct of its operators, instead of the contracting integrity of its suppliers, occurred when the costs reached the level of a major bilateral relationship. A single case suggests that such a threshold exists, and 3.2 sets out why even that case allows a second reading. It does not fix where the threshold sits, and it does not establish that comparable costs applied again would reach it. Caution about predicting the PRC's reaction applies both ways: to observed correction and to observed non-response. The conclusion therefore indicates a direction only: **a response set that stops well below the only level at which correction has ever been observed is unlikely to reach it.**

Three components would raise the level at which the response operates, and each depends on the others. First, the record has to be treated cumulatively rather than incident by incident. Court-authorized disruptions and sanctions designations already generate evidence under judicial and administrative standards, and that evidence is currently distributed across the jurisdictions that produced it. Consolidating it into a standing, shared record of PRC cyber campaigns converts a series of separate cases into a documented pattern.[309] A pattern supports the argument that a state has built and sustained a system, and it is what allows a response to be calibrated to a decade of conduct instead of only to the operation most recently discovered.

Second, coordination has to be structured so that speed is not sacrificed to unanimity. The instruments exist. For example, the EU's Cyber Diplomacy Toolbox, adopted in 2017 as a framework for a joint diplomatic response to malicious cyber activities and revised in 2023, sets out the graduated measures available, and the restrictive-measures regime established in 2019 gives the most consequential of them legal form.

The March 2026 listings show that this framework works against PRC-nexus entities and individuals. What limits their effect is the decision rule rather than the toolkit: restrictive measures are adopted under the common foreign and

309 Christina Rupp and Alexandra Paulus (2023): Official Public Political Attribution of Cyber Operations – State of Play and Policy Options & interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop

security policy and therefore require the agreement of every member state.[310] The constraint is procedural rather than legal. Where a response requires the agreement of every member, the state least willing to act determines the pace, and adversaries have an incentive to cultivate that state to do their bidding. The constraint is acknowledged from inside the institution. In September 2026 the European Commission President told the European Parliament that Europe's doctrine, institutions and decision-making had not kept pace with the new reality, that they had been built for a different world, and that a system driven by attempts at consensus and compromise may no longer be fit for purpose.[311] The criticism therefore comes from the Union's own executive. A senior NATO official has argued that costs should be imposed on adversaries for cyber campaigns and other hybrid activity even where doing so means working around consensus requirements, on the reasoning that fragmented responses are what adversaries seek to exploit.[312] The practical form this takes is a coalition of willing states acting in parallel and on a common evidentiary basis, with those unwilling to act declining to join instead of blocking the response. **A coordinated response by a subset of affected states imposes more cost than a unanimous response that arrives too late or not at all.**

Third, the costs have to be visible outside the cyber domain. The PRC has absorbed consequences that stayed within it. **Diplomatic, economic, and informational instruments reach interests that operational infrastructure does not, and they carry the further advantage of being visible to audiences inside the PRC and to third states, which consequences delivered through classified channels are not.** Others make the same case. A September 2026 assessment from the CFR recommends preparing a menu of consequences outside cyberspace – structural sanctions on state security and military entities, secondary sanctions on those who support them, export controls, visa restrictions, and coordinated allied measures – and concludes that changing PRC conduct requires making cyber campaigns

310 Council of the European Union (2026): Sanctions against cyber-attacks & Council of the European Union (2019): COUNCIL REGULATION (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States & Council of the European Union (2026): Cyber-attacks against the EU and its member states: Council sanctions three entities and two individuals & Council of the European Union (2017): Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") - Adoption

311 European Commission (2026): 2026 State of the Union Address by President von der Leyen

312 Ido Vock (2026): Senior Nato official calls for stronger response to cyberattacks

a priority issue in the US–China relationship.[313] The reasoning that leads there differs from the reasoning set out here. That assessment treats the contractor layer as a feature that complicates attribution and allows rapid reconstitution. The assessment offered here is that the central government could correct and does not, which is why the response has to reach the state, not only the operators. **This is not a recommendation to escalate. It is a recommendation to apply, in a coordinated and cumulative way, instruments such as economic sanctions that affected states already hold and already use in other policy areas.**[314] Linkage of this kind is already routine in US–China relations. Both governments have used rare earths, semiconductors, agricultural purchases and military exercises as leverage on unrelated issues. Cyber conduct has so far not been part of that bargaining.[315]

One constraint applies to all three components, and such arrangements have failed on it before. The states with the greatest exposure to PRC cyber campaigns are frequently the states with the greatest economic dependence on the PRC, and that dependence is asymmetric within any coalition.[316] **The PRC can therefore apply economic counter-pressure selectively, against the most exposed participant rather than against the coalition as a whole.**

The constraint reaches further than coalition politics. Reporting in 2023 described a multi-year campaign against eight Kenyan ministries, including the presidential office, assessed as seeking insight into the government's capacity to service debt incurred under Chinese-financed infrastructure programs. The Kenyan government did not treat the reporting as an attribution to be considered. It rejected it publicly, and the argument offered was that most of the state's networking infrastructure is supplied by the PRC, so that a state wishing to enter those systems would have had no need of contractors.[317] Where dependence runs deep, it does more than weaken a collective response: it keeps the affected state out of the coalition from the start.

---

313 Matthew Ferren, Adam Segal, and Rush Doshi (2026): The Cyber Gap – How to Counter China's Threat to America's Critical Networks Xi's state visit to Washington in September 2026 ended with tariff cuts, coal purchases and a channel for incidents involving AI. Neither government's list of outcomes mentions cyber, see The White House (2026): Fact Sheet: President Donald J. Trump Advances a Fair and Reciprocal Relationship with China While Hosting Historic State Visit

314 Compare for example Ama Lotlana (2026): The EU's 21st Sanctions Package: China's Retaliation and the Limits of European De-Risking & Giorgio Leali (2026): 5 EU countries call for tougher trade weapons to tackle China

315 Adam Segal and Matthew Ferren (2026): Changing China's Cyber Calculus

316 European Commission (2023): Protecting against coercion & Rob Joyce (2026): China's Cyber Explosives are in Place. Where's our Response?

317 Reuters (2023): Chinese hackers attacked Kenya State agencies & Beth Nyaga (2023): Kenya: Reuters report on Chinese hackers is sponsored propaganda

A collective response that does not include a prior commitment among participants to share the cost of counter-pressure is unlikely to survive the first application of it. Such commitments can be made. Chinese trade measures against one EU member state over its handling of relations with Taiwan are the case most often cited as what economic coercion against the Union looks like, and the EU adopted an instrument in 2023 allowing it to respond collectively where a third country applies or threatens trade measures against a member state to force a change in policy.[318] The Anti-Coercion Instrument was designed to require only a qualified majority to be triggered, precisely to avoid a single state blocking action. The first case came in January 2026, from the US. President Trump threatened eight European countries, Denmark among them, with tariffs unless the US could buy Greenland. France called for the instrument to be used, and one EU diplomat said the qualified majority would be reached. Member states still held back to give talks with Washington a chance.[319] Three days later, the US dropped the threat.[320] What held the Union back was the reluctance of member states to risk an escalation, and a lower voting threshold does not remove that. A prior commitment to share the cost of counter-pressure is meant to address exactly this.

6.5 Ceiling Contingency

The ceiling – no campaign aimed at disrupting the operation of critical infrastructure – rests mainly on the fact that no such campaign has been observed. Restraint is likely part of the explanation. Two others are possible: in some cases the access may not have been complete enough to disrupt operations, and in others the operation may have had a different aim. Known cases are few, and much of the incident response and technical detail is not public. What can be observed is that capability is present and that access has been held for long periods in power, water, and transport systems. No contingency has yet arisen in which disrupting the operation of foreign critical infrastructure would have served a Chinese objective, so whatever restraint there is has not been tested under the conditions that would matter. Affected states should therefore not plan on the assumption that, because no PRC campaign has so far aimed at disrupting critical infrastructure, none will. **Access that PRC actors hold in critical infrastructure should be treated as access they may one day use to disrupt it.** States should prepare for that case, alone and together, in three ways.

---

318 Chloé Bamberger (2026): EU weighs first activation of Anti-Coercion Instrument amid Trump tariff threats & European Commission (2023): Protecting against coercion

319 Maria Tadeo and Mared Gwyn Jones (2026): EU holds back trade 'bazooka' as it seeks diplomatic solution with the US over Greenland & Maria Tadeo (2026): EU seeks Greenland de-escalation while plotting tariff retaliation against Trump

320 John Power (2026): Trump drops tariff threat, says he won't take Greenland by force

First, continuity planning in critical infrastructure already covers deliberate attacks, including cyber operations, and should be extended to the specific case of an adversary that has prepared in advance.[321] The joint assessment underlying the relevant advisories is that the actors involved are collecting access in infrastructure in order to enable movement into operational assets and to disrupt functions in the event of a major crisis.[322] In the sectors where such access has been found, continuity planning should therefore assume an adversary that is already present, that selects the moment, and that may reach the recovery path as readily as the primary system. This means restoring systems without relying on trusted networks, providing manual fallback for processes that depend on compromised control systems, and running exercises that rehearse operation under those conditions. This work is slow, and it cannot be started once a contingency has begun.

Second, the EU has a framework for managing such an event, but not for answering it. The European Union adopted a blueprint for cyber crisis management in 2025 that sets out roles across the crisis lifecycle and a shared severity scale, but it governs detection, coordination and recovery, not what the responsible state would face, and it is non-binding.[323] The gap is now recognized at the highest level of the Commission. In her State of the Union address of September 2026, the Commission President said the European Union needs its own counter-hybrid playbook, and proposed an Emergency Security Protocol that any member state could trigger, convening all member states to coordinate a response, deter further escalation, and limit the damage.[324] The proposal was made with Russian sabotage and drone incursions in mind, but it is defined by threshold instead of by adversary: incidents that fall below armed aggression and still threaten national security, including cyber operations. A Chinese cyber campaign that disrupted the operation of critical infrastructure would sit inside that definition.

However, the mechanism is a proposal and not an agreed instrument, so it does not yet close the gap. And it only offers a way to meet. It does not decide what to do then, which is the harder question and should be settled in advance.

---

321 European Union (2022): Directive (EU) 2022/2555 (NIS2) & European Union (2022): Directive (EU) 2022/2557 (CER)

322 Cybersecurity & Infrastructure Security Agency (2024): PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

323 Council of the European Union (2025): EU adopts blueprint to better manage European cyber crises and incidents

324 European Commission (2026): 2026 State of the Union Address by President von der Leyen

Third, as far as the absence of such campaigns reflects a choice, that choice depends on what the PRC expects the consequences to be. Stating jointly and publicly what a campaign aimed at disrupting critical infrastructure would bring is the least costly measure available to affected states, and the only one in this set aimed at preventing such a campaign. The idea is not new. The EU's framework for a joint diplomatic response rests on the proposition that clearly signaling the likely consequences of such a response influences the conduct of potential aggressors.[325]

Two caveats apply. First, declaratory signaling has a weak track record against this particular adversary. Costs that were imposed and made public have been absorbed and not answered with restraint, which is a reason to treat the measure as low-cost and possibly useful, but not reliable.[326] Second, and more importantly, a threshold stated only at the level of operational disruption risks conceding everything beneath it. The May 2020 case in Taiwan, in which access held for months inside a state-owned petroleum company was executed against payment and business systems while production was left untouched, indicates calibrated use rather than abstention.[327] An adversary that can disrupt business systems while sparing operations can easily stay just below a line drawn at operations. A declaratory position should therefore address the holding of persistent access in civilian systems, and not only its execution. It should also cover disruption caused by ransomware used as cover, since the effect on the operator may be the same. The authors of the CFR assessment reach the same position, proposing that Beijing be told that holding access in civilian infrastructure would draw consequences outside cyberspace.[328]

6.6 Record Consolidation

Four of these measures depend on the same thing: a shared record. Collective cost imposition is applied on an accumulated record. Attribution at the level of firms, universities, and tasking bureaus requires that record to be maintained instead of assembled after each discovery. Assigning responsibility to the state as a default depends on a documented pattern rather than on a documented operation. A

325 Council of the European Union (2019): COUNCIL DECISION (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

326 Chris Bing (2018): Trump administration says China broke Obama-Xi hacking agreement & John W. Rollins (2015): U.S.-China Cyber Agreement

327 Unnamed (2020): Bureau names ransomware culprits & Sean Lyngaas (2020): Taiwan suggests China's Winnti group is behind ransomware attack on state oil company & Trend Micro (2020): Targeted Ransomware Attack Hits Taiwan Organizations

328 Adam Segal and Matthew Ferren (2026): Changing China's Cyber Calculus

response agreed before a ceiling breach requires an evidentiary threshold settled in advance, which presupposes a body of evidence against which such a threshold can be set. The measures can be carried out separately, but all of them need the record.

That record does not currently exist in a usable form even though the material is largely public, ranging from court-authorized disruptions, sanctions designations, indictments and joint advisories to the technical reporting that accompanies them. What is missing is bringing it together. The evidence sits in the jurisdiction that produced it, in the format that the jurisdiction uses, at the moment that jurisdiction chose to release it, and it is assembled anew by whichever government next needs it. **A decade of documented conduct is available and is being used one incident at a time.**

Such a record has to meet four requirements. First, it has to be continuous instead of episodic, since a pattern builds up over time, and a record put together for one decision will look as if it was made to justify it. Second, it has to be built to a published standard, so that entries can be either corroborated or contested on their evidentiary basis rather than on the motives of whoever compiled them, and so that a government relying on it can say what it is relying on. A published standard governs how entries are judged. It does not change what is entered in the first place: which campaigns governments attribute depends on political considerations, and which campaigns vendors report depends on what they can see.[329] The record can therefore document a pattern of conduct. It cannot serve as a complete count, comparisons between states drawn from it need care, and each entry should show where it came from. Third, it has to be sufficiently independent of any single government that its findings survive a change of administration in any one of them. This is a practical need: a record that lapses when its main sponsor loses interest cannot support commitments made years in advance. Fourth, it has to be understandable for those who would use it: foreign ministries, legislatures, and regulators as well as threat intelligence specialists.[330]

Whether such a record is maintained by affected states jointly or by an independent body serving them is a question of institutional design. Either way, a response calibrated to a pattern requires the pattern to be documented, and at present each government documents its own share of it and then puts the file away.

---

329 Florian Egloff and Max Smeets (2023): Publicly Attributing Cyber Attacks: A Framework

330 interface (2026): Primary research with practitioners and researchers from the Transatlantic Cyber Forum working group on "Irresponsible Behavior During Cyber Operations" through a survey, interviews, and a workshop & Christina Rupp and Alexandra Paulus (2023): Official Public Political Attribution of Cyber Operations – State of Play and Policy Options

6.7 Resilience

Resilience sits apart from the other measures. Since the PRC has largely absorbed the costs imposed so far, resilience is the one part of the response that pays off whatever Beijing decides – and one a state can start without a partner.

Resilience and cybersecurity are often used interchangeably, although they answer different questions. Cybersecurity measures aim to prevent a compromise from occurring. Resilience assumes that one has occurred and works to keep the resulting damage as small as possible and bounce back as fast as possible.[331] Against an adversary that holds access quietly for years, using tools already present on the system, that assumption fits.

Resilience also pays off unevenly across the PRC ecosystem, and that works in the defenders' favor. The quality of Chinese operations spans a wide range, from a disciplined elite at one end to a tolerated stream of loose contractor work at the other. Against the loose end, ordinary operational security and resilience measures are largely sufficient. Operators that reuse public proof-of-concept code within hours of disclosure are defeated by timely patching. This reaches well beyond the sectors the PRC prioritizes. A campaign that compromises broadly first and selects afterward hits any system that is exposed and unpatched, whether or not its owner would ever be chosen as a target. Operators that reuse shared tooling which others have already had analyzed are caught by conventional detection. Operators that blend state tasking with financially motivated crime generate the kind of noise that monitoring is designed to identify. Against the disciplined end, none of this suffices, and active threat hunting is required.[332] As a result, the same investment removes much of the volume and reduces what remains to a problem small enough to hunt.

Affected states should be able to show four capabilities: anticipation, the ability to withstand a compromise, recovery, and adaptation.

Regarding anticipation, persistent access to systems cannot be found by waiting for alerts, since advanced tradecraft is designed to produce none. What it requires instead is threat hunting that starts from the assumption that an intruder is already present and works to disprove it, concentrated where access collection and long-term intelligence collection are most likely. The PRC's own plans point

331 Sven Herpig (2023): Mehr Resilienz für Deutschlands IT-Systeme

332 Sven Herpig (2022): Cybersicherheitspolitik: Deutsche Ideenlosigkeit?

to where that is. The industrial, technological, and infrastructure priorities of the successive Five-Year Plans offer a published, if partial, targeting forecast: observed intrusions have tracked them closely, though provincial and emerging priorities shape targeting as well.[333] Affected states should treat infrastructure operators, and the sectors named as strategic in the current plan[334], as standing priorities for threat hunting. Findings should be shared across allied response teams, so that a technique exposed in one country is denied in the others.[335] This approach has already worked: collected access in communications, energy, and transportation systems has been found by defenders working from the assumption of compromise instead of from alerts, in environments where conventional detection had reported nothing.[336]

Regarding the ability to withstand a compromise, the objective is not an intrusion that causes no harm, but critical processes that continue to run while the intrusion is dealt with. Network segmentation limits how far an intruder already inside the network is able to travel, which bears directly on access collection, since access to an office network is of value only if it leads somewhere. Intrusion detection shortens the interval before the compromise is noticed. Tested incident response plans determine whether the first hours are spent containing the compromise or establishing who is responsible for doing so. Analog fallback belongs here too: a process that can run on paper while systems are down has not stopped.

Regarding recovery, the restoration of function begins with the processes that matter most and depends on preparations made long beforehand. Backups that have been tested by restoring from them, (geo-)redundant infrastructure able to carry the load, and a plan for clearing the compromise out largely determine whether an outage is measured in days or in weeks. Clearing out has to cover credentials and certificates as well as implants. When a PRC-linked group was removed from the network of a company serving the UK government in 2017, it was soon back inside, logging in through the company's VPN with a certificate taken from one of the machines it had compromised.[337] Recovery also decides what a breach of the ceiling would cost in practice: the faster a system comes back, the less disrupting it is worth.

---

333 Sveva Vittoria Scenarelli (2026): Understanding modern Chinese cyber operations means shifting from 'APT' to composite responsibility

334 Natto Team (2026): Cybersecurity Strategy in China's 15th Five-Year Plan

335 Bundesnachrichtendienst (2025): Joint Cybersecurity Advisory – Gemeinsamer Sicherheitshinweis zu staatlich geförderten chinesischen Akteuren (Cyber-Akteur SALT TYPHOON)

336 Cybersecurity & Infrastructure Security Agency (2024): PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

337 Eduard Kovacs (2018): China-Linked Spies Used New Malware in U.K. Government Attack

Regarding adaptation, the vulnerabilities that were exploited should be closed, and what an incident has revealed should change how the first three capabilities are performed. Patch management belongs here, and is the kind of routine work that is often deferred. Together with strong credentials and multi-factor authentication, it is also one of the measures that most reliably remove the access route on which the opportunistic layer of the ecosystem depends. Patching has a limit: it needs a patch to exist. In a test setting, teams of AI agents have exploited real vulnerabilities without being told what the flaw was, and PRC actors are already building AI into their operations (2.5).[338] Adaptation therefore also has to prepare for flaws that have no fix yet, by reducing what is exposed to the internet, limiting how far a single flaw can reach, and detecting and containing intrusions faster than staff could on their own. A recent evaluation of AI agents for automated defense, run in a simulated network, found them competitive but too variable and too slow for some real-world uses.[339]

Two considerations should govern an affected state's decision to accelerate funding for this work. First, resilience is threat-agnostic. The same segmentation, backups, and response plans that limit a PRC state-sponsored intrusion also limit activities by other nation states, criminal ransomware, a failed migration, or a flood. None of the remaining six measures discussed throughout this chapter produces a comparable return if the assessment set out here proves mistaken. Second, resilience requires no partner. Collective cost imposition faces two constraints: short of extreme events, a coalition has to be built anew for each case, which takes time (4.4), and once built, it tends to break at the member most exposed to the PRC economically (6.4). Resilience is subject to neither. It does not depend on unanimity, on a partner willing to share the cost of solidarity, or on how the PRC government chooses to respond, and it can be begun by a single state at once.

Resilience is also the only measure whose progress can be checked directly. Whether a coordinated response has changed the PRC's conduct is a judgment that can be made only years afterward. Whether a data center is able to restore its systems from backup can be established within the current quarter.

For affected states, the difficulty lies in implementation. Germany's federal court of auditors reported in 2025 that federal data centers frequently lacked operating redundancy and functioning, tested backup processes, and concluded that federal

338 Yuxuan Zhu, Antony Kellermann, Akul Gupta, Philip Li, Richard Fang, Rohan Bindu and Daniel Kang (2026): Teams of LLM Agents can Exploit Zero-Day Vulnerabilities

339 Thibaut Jacques (2026): A systematic evaluation of large language models for autonomous cyber defense

infrastructure was not prepared for current threats.[340] The finding describes a pattern visible well beyond one country: strategies, policies, and regulations are adopted more quickly than they are implemented, institutions are established more quickly than they are staffed, and prestige projects are funded ahead of the personnel who configure firewalls and test backups.[341]

In sum, resilience shows the same pattern as the rest of the response: the instruments to impose costs exist but are not used effectively, and the obligations to reduce returns exist but are not funded.

340 Bundesrechnungshof (2025): Cybersicherheit Weichenstellungen für einen sicheren Cyberraum

341 Sven Herpig (2025): Operative IT-Sicherheit stärken statt Strategiepapiere stapeln

7. Conclusion: The Delegation Is The Policy

The PRC's cyber campaigns are widely read as being run by an ecosystem that the government in Beijing no longer fully directs. A senior FBI official has said so publicly, and indictments have called the system reckless and indiscriminate. The record supports a different reading. The central government has not lost control of its cyber campaigns. It tolerates the looseness they produce, as the price of operating at scale.

That conclusion rests on two things: what the state has built, and what it declines to fix. Over more than a decade the PRC put in place the legal obligations, institutional pipelines, force structure, and talent base needed to run operations at volume, and drew on commercial supply markets that grew alongside them. Reporting duties route vulnerabilities to the state, and the same rules restrict how they may flow outward. Competitions and universities identify talent. Initial access, covert infrastructure, and tooling are often bought, sold, and shared.

Within that structure, control is high at the core where the central government sits and loose at the edge where contractors and other third parties sit. Contractors act on their own initiative, and espionage and financially motivated crime blend into each other, with neither drift corrected. Some tools spread after deployment and are left to spread. The correction record shows that the PRC could correct these patterns and chooses to tolerate them instead. Debarments corrected how contractors bid for contracts but not how they operate, and enforcement against cyber-enabled fraud shows that the state can correct at scale. A state that can correct and does not has made a choice. The ceiling – no campaign aimed at disrupting the operation of critical infrastructure – has held so far, but it has not been tested.

Responsibility follows from the system the state built. It does not depend on individual instructions. A state that builds an execution layer, declines to correct how it runs, and keeps buying what it produces bears no less responsibility than one that has genuinely lost command of it. Whether the state ordered a specific intrusion only shows how the campaign was run. It does not limit the state's responsibility.

For affected states, this means that dealing with PRC cyber operations is a cost problem, not a capability problem. They already hold the instruments to raise

what these campaigns cost the PRC. What has kept the costs to Beijing low is how those instruments have been used. The costs imposed so far have been absorbed. PRC activity stays below the level that would trigger a decisive political response. Responses mostly address single incidents and rely on technical instruments, instead of the economic and diplomatic channels to which the PRC has reacted in the past.

The seven measures set out here answer those shortcomings. Two deny the benefit, four impose the cost, and the seventh – a consolidated record of conduct that is already documented – is the condition others depend on. None of the seven requires new legal powers.

Three developments would show that the assessment of the PRC's cyber campaign ecosystem, or the conduct it describes, has changed. The first would be the central government correcting how its operators behave in the field, as distinct from the contracting misconduct it already polices. That would show the boundaries of what is tolerated narrowing, and delegation being reined in. The second would be a PRC campaign aimed at disrupting the operational functions of critical infrastructure. That would cross the ceiling, and would change the calculation behind every response. The third would be a change in operational behavior after a group of affected states imposed costs together – a measurable drop in tempo, a narrowing of targeting, or a visible tightening of tradecraft in the months after a coordinated response package, as bilateral pressure briefly produced after the 2015 agreement on commercial cyber espionage. The distinction matters, because the instrument this tests has not yet been applied at that scale. Watching for the third development makes the cost-imposition measures testable. No change would be as telling as a change.

Until one of these developments is observed, the position stands as set out: **The PRC built up the system, tolerates how it runs, and keeps buying what it produces. The delegation is the policy, and affected states are entitled to respond to it as such.**

Appendices

I. Research

In January 2025, interface started to set up an international and interdisciplinary working group made up of 38 practitioners and researchers working on various topics within the field of cybersecurity. Members were recruited from 150 alumni of the Transatlantic Cyber Forum (TCF) founded in 2017 and beyond to form the "TCF working group 'Irresponsible Behavior During Cyber Operations,' with a particular emphasis on state-backed Chinese campaigns".

In parallel with the obligatory desk research (cut-off date: October 15, 2026), 23 semi-structured interviews on the topic of Chinese cyber campaigns were conducted with members of the working group between January and May 2026.

In February and March 2026, an expert survey was conducted on the topic of "Chinese level of control over cyber operations" with 23 respondents.

On May 11–12, 18 members of the working group came together from five continents for a two-day interactive workshop in Bonn to discuss "Chinese Cyber Campaigns Out Of Control?".

The draft policy paper, developed based on the knowledge and insights from desk research, interviews, survey responses, and workshop interactions in July and August, was reviewed in September by 18 members of the working group and additional reviewers.

II. Acknowledgments

This analysis was supported by the Transatlantic Cyber Forum working group on “Irresponsible Behavior During Cyber Operations”. The views and opinions expressed in this paper are those of the author and do not reflect the official policy or position of the working group members or that of their respective employer(s). In alphabetical order, the author acknowledges the essential contributions of the following individuals:

1. Charles-Pierre Astolfi, IGN
2. Eugenio Benincasa, ETH Zürich
3. Antonia Bulfon, Institute for Peace Research and Security Policy
4. Mei Danowski, Natto Thoughts
5. Francis C. Domingo, University of the Philippines Diliman
6. Finn Hagemann
7. Omolara Esther Hamzat
8. Antonia Hmaidi, Mercator Institute for China Studies (MERICS)
9. Sherry Huang
10. Joanna Kulesza, University of Lodz
11. Nicholas Leiserson, Institute for Security and Technology
12. Igor Mikolic-Torreira, Center for Security and Emerging Technology (CSET), Georgetown University
13. Aleksandar Milenkoski, SentinelLABS (SentinelOne)
14. Dai Mochinaga, Shibaura Institute of Technology
15. Lukasz Olejnik, independent consultant / King’s College London
16. Pavlina Pavlova, Critical Cyber
17. Thomas Reinhold, PRIF – Peace Research Institute Frankfurt
18. Sveva Vittoria Scenarelli
19. Fernando Sol III
20. Aleksandra Sowa, FG PET – German Informatics Society
21. Timo Steffens, Federal Office for Information Security (BSI)
22. Nakshathra Suresh
23. Eric MSP Veith, OFFIS – Institute for Information Technology
24. Julian-Ferdinand Vögele, Recorded Future
25. Valentin Weber, German Council on Foreign Relations (DGAP)

The author extends special gratitude to the entire Cybersecurity and Emerging Threats team at interface, Luisa Seeling and Alina Siebert, as well as Claude [Anthropic’s AI] and Jade [interface’s AI] for their assistance with editing and laying out this publication.

This project was made possible by the generous support of the German Federal Foreign Office. The views expressed in this paper do not necessarily represent the official position of the ministry.

About the Author

Dr. Sven Herpig

Dr. Sven Herpig is interface's Lead Cybersecurity & Emerging Threats and Advisor to the Executive Director. He analyzes the roles of government in various areas of cybersecurity policy, including Chinese cyber threats, operational parameters of cyber campaigns, responses to cyber operations, the use of agentic AI in cyber operations, vulnerability management, securing machine learning, and fostering open source software security.

Contact

Dr. Sven Herpig
Lead Cybersecurity & Emerging Threats | Advisor to the Executive Director
sherpig@interface-eu.org
+49 (0) 30 81 45 03 78 91
bsky.app/profile/z-edian.bsky.social
github.com/z-edian/publications

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org

T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
Ebertstraße 2
D-10117 Berlin

Layout by Thorsten Kirchhoff
Infographics by Alina Siebert

Corporate Design by Make Studio
www.make.studio

Code
Convoy Interactive

This paper is published under Creative Commons License (CC BY-SA). This allows for copying, publishing, citing and translating the contents of the paper, as long as interface is named and all resulting publications are also published under the license “CC BY-SA”. Please refer to creativecommons.org/licenses/by-sa/4.0/ for further information on the license and its terms and conditions.