DARKTRACE

Crimson Echo: Chinese Cyber Tradecraft as Strategic Statecraft

Long-term operational evidence and implications for the West

Darktrace's Chinese-nexus investigative report, "Crimson Echo: Understanding Chinese-nexus Cyber Tradecraft Through Behavioral Analysis," is based on a long-term review and threat hunt for evidence of cybersecurity incidents involving Chinese-nexus threat actors across the customer base since mid-2022.

The report illustrates that Chinese-nexus cyber activity is ingrained in strategy, doctrine, and statecraft.

Key takeaways include a clear Chinese-nexus operator decision model that is articulated in the fully detailed report, tradecraft constants (observed patterns over years), and variables, with drawbacks that include assumptions, limitations, and lessons learned.

Executive Summary

This report set out to answer two simple, but often not fully addressed questions:

01 What does sustained Chinese-nexus cyber activity tell us about tradecraft, operational cadence, priorities, strategic intent, and future risk?

02 What does Chinese-nexus cyber activity look like in a way that's digestible and beneficial for different stakeholders (i.e., CEOs, CISOs, analysts, government)?

Key insights:

- Chinese-nexus cyber operations are best understood as continuous strategic planning, not episodic campaigns.
- Detection of short dwell time intrusions should not be interpreted as tradecraft failure but deliberate operational choices.
- Western security models remain overly incident-centric and systemically undervalue persistent identity risk.
- China's cyber activity is not just focused on IP theft but increasingly aligns with Belt and Road Initiative (BRI) dependencies and critical infrastructure leverage globally, particularly in the United States.

None of these observations are individually novel. Treating them as a coherent operational system with long-term implications provides opportunity for the West. Across three years of investigations and dozens of confirmed cases, the most consistent finding was not a specific tool, vulnerability, or campaign, but rather distinct modes of operation.

Chinese-nexus cyber tradecraft, as evidenced in the report, reflects a long-term approach that values access as an asset, restraint as a strategy, and optionality as a source of leverage. Recognizing this doesn't require alarmism, but it does necessitate a shift in how risk is conceptualized and addressed.

Understanding Historical Chinese Tradecraft

China's cyber ecosystem has evolved much like its economy has: rapidly and at scale. This has been achieved through a myriad of ways but guided by its 5-year phased plans. Therefore, it seems suitable to discuss Chinese-nexus cyber tradecraft in phases. These phases are for analytical constructs, not formal Chinese doctrine and reflect shifts observed across reporting [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

Phase 1: Late 1990s to early 2000s

- Informal patriotic hacker groups
- Low sophistication, high volume
- Highly visible activity focused on symbolic targets

Phase 2: Mid-2000s to early 2010s

- Early APTs identified (i.e., Mandiant APT 1 report)
- Gradual but slow state integration
- Economic espionage and IP theft
- Increased sophistication in tooling and infrastructure reuse
- Clear malware and infrastructure patterns

Phase 3: Mid 2010s to 2020

- Ministry of State Security (MSS) as puppeteers of nexus operations
- Increased West attribution
- Faster tool turnover, infrastructure diversity, reduced tool reuse
- People's Liberation Army (PLA) internal cyber restructure with military-civil fusion focus
- Access scalability
- Focus on managed service providers, supply chain, third party access
- Offensive cyber growth in private sector blurs attribution lines and increases state plausibility

Phase 4: 2020 to Present

- Identity oriented (SaaS, MSP, telco)
- Network edge focus
- 'Smash and grab' for quick wins/(IP theft, proxy set up)
- Increased BRI cohesion
- Higher operations security (OPSEC)
- Living-off-the-land
- Persistent low-tempo and access maintenance;
- Access as a strategic asset
- Hold critical infrastructure at risk

Chinese-Nexus Operator Decision Models

Across the Darktrace investigative dataset, intrusion tempo and operational security varied markedly by target type. Analysis of the dataset indicates two distinct operator models rather than a single continuum of tradecraft maturity.

The first category consisted of short-dwell "Smash and Grab" activity, which was frequently observed with the first three to four days of access and characterized by rapid escalation, over tooling, and limited concern for long-term stealth. Intrusions appeared time bound for credential harvesting, reconnaissance, or to enable follow on activity elsewhere.

A secondary category of "Low and Slow" activity emerged around the ten-to-fourteen-day mark, where operators appear to evaluate access and target relevance. Activity during this period was intermittent, reduced tool footprint, and identity centric.

Intrusions involved demonstrated substantially longer dwell times and higher operational security. Extensive use of legitimate administrative mechanisms, long periods of inactivity, redundant access paths, and no visible exfiltration were observed.

The observed "low and slow" behaviour model in these environments is consistent with nation-state access being considered a strategic asset.

"Smash and Grab" aka B2E: Breach→ Burst→ Exit

Breach: Gain access fast, not quietly; often leverages exposed services and recently disclosed vulnerabilities, reused credentials; detection risk acceptance.

Burst: Maximize access before degradation; rapid privilege escalation; internal recon; semi-custom, commodity tooling; reused across targets

Exit: Leave before return diminishes, little or no attempt to clean artifacts; burn accepted

Key decision drivers: optimize speed and scale, accept burn

"Low and Slow" aka P³O Position → Prove → Preserve → Orchestrate

- **Position:** Establish stable, low-noise access prioritising identity and persistence.
- **Prove:** Validate strategic value and access quality through restrained exploration.
- **Preserve:** Maintain access as an asset with redundancy and minimal interaction.
- **Orchestrate:** Pivot access when conditions or objectives shift without restarting operations.

Key decision drivers: strategic value, access fragility, geopolitical timing.

Tradecraft Constants and Variables

Constants	Variables
Identity-centric access	Initial access vector
Redundant persistence	Malware and tooling
Operational restraint	Infrastructure and C2
Target-driven investment	Cloud vs on-prem focus
Rapid or low operational tempo	Level of interaction and automation

The same operational ecosystem can employ both models concurrently, selecting the appropriate model based on target value, urgency, intended access. The observation of a "Smash and Grab" model should not be solely interpretated as a failure of tradecraft, but instead an operational choice likely aligned with objectives. Where "Low and Slow" operations are optimised for patience, "Smash and Grab" is optimised for speed; both are seemingly deliberate operational choices, not necessarily indicators of capability.

	"Smash & Grab" (B2E)	"Low & Slow "(P^3O)
Perceived Value	Immediate	Long Term Option
Access	Consumable	Strategic
Time Horizon	Days	Weeks- Months - Years
OPSEC Priority	Low-medium	Very high
Persistence	Minimal	Redundant
Tooling	Commodity/Semi custom	Legit admin/LOTL
Typical Targets	Commercial, Suppliers	Critical Infrastructure
Detection Tolerance	High	Very Low

China's 15th Five-Year Plan and 'China 2030' Strategic Direction

China's 15th Five-Year Plan reinforces indigenous innovation and core technology breakthroughs around AI, semiconductors, and advanced materials with strong emphasis on innovation capacity, deep integration of science, and industry. With technological reliance as its core message, cyber and digital domains will likely remain integral to broader national goals supporting acceleration, acquisition, and protection of technologies that underpin national power. From this perspective, Chinese-nexus cyber tradecraft should not be viewed as siloed activity but an extension of long-term strategic planning [11][12][13][14].

Western Failure Taxonomy

The Crimson Echo findings highlight a few challenges to current approaches widely used in Western cyber defense operations [15] [16]. These challenges are not unique to any one country — they are structural issues across Western enterprise and government networks. These include:

- **Strategic:** treating cyberspace and cybersecurity as episodic incidents rather than continuous competition.
- **Cognitive:** overreliance on known indicators, assuming that low-volume signals low threat, misreading quiet persistence as low risk, bias towards familiar intrusion patterns.
- **Organisational:** a disconnect between public policy, board understanding, and operational cyber realities, unclear IT/OT ownership, compliance-driven security.
- **Operational:** alert fatigue, volume without context, insufficiency in telemetry and retention, poor identity lifecycle management and hygiene.
- **Architectural:** legacy infrastructure, flat networks, over-privileged identities, rapid cloud sprawl without governance, edge/IoT/remote access technologies functioning without secure by design principles.

For example, a recent Darktrace-observed Salt Typhoon intrusion on a European telecom operator was due to the exploitation of a known vulnerability [17][18][19].

The observed intrusion succeeded less because of adversary brilliance but instead more likely because of recuring blind spots and weaknesses. This pattern is not anomalous, but representative.

Implications for Western Security Policy

Chinese-nexus cyber activity is often evaluated through the lens of incidents, breaches, or campaigns. The observed operator models in the Chinese cyber ecosystem functions as strategic leverage (20).

While tooling, infrastructure, and initial access vectors continue to change, the persistence of identity-centric access, redundant footholds, and operational restraint suggests that Western defenses overly focused on malware and indicators will remain structurally misaligned.

Until Western security models evolve from an immediate focus on incident response and threat intelligence to a long-term emphasis on access governance, this asymmetry in cyberspace will persist – regardless of tooling, attribution, or public exposure – and remain a Chinese strategic asymmetric advantage in statecraft.

This doesn't make defense futile, but it does change what good defense looks like. Below are a set of recommendations that could provide a starting point for evolving Western cyber defense and aproaches [21] [22] [23] [24] [25] [26].

- **Shift** metrics from incidents to access risk.
- **Treat** identity providers as critical infrastructure.
- **Mandate** telemetry and retention standards.
- **Strengthen** telecom and cloud dependency governance.
- **Expand** supplier and integrator oversight.
- **Institutionalize** red-team validation.
- **Expand** incident response tabletop exercises, exercise quiet leverage crisis scenarios.
- **Invest** in rapid containment capabilities.

Anticipated convergence between China's 15th Five-Year Plan and Western technological trajectories is likely to create several strategic inflection points.

As identity systems and cloud architectures merge, they will increasingly shape control planes, persistent access pathways, and supply-chain leverage—surpassing the importance of direct targeting. Cyber access will function as a long-standing strategic asset, reinforced by AI-enhanced tradecraft.

As a result, cyber risk will shift from isolated incidents to systemic exposure, pushing defenders to move beyond reactive approaches toward continuous exposure management, behavioral-led detection, and rapid containment. These inflection points reflect a synthesis of public intelligence reporting, national cyber advisories, long-term vendor investigations, evidence of persistent access operations, identity-centric tradecraft trends, and the integration of cyber capabilities into broader state-level strategic competition.

Appendix 1: Methodology Limitations

While the findings of "Crimson Echo" are robust, they are constrained by the scale and structure of the underlying dataset. In total, low-medium-high cases over the last 3 years reflects upwards of 80 at the time of writing. The meta model and subsequent analysis were restricted to the more than 50 cases deemed medium to high confidence, which provides its own challenge of both mistaken observations and analysis omittance.

This limits statistical power and means the results should be treated as descriptive rather than definitive. Summary statistics, bootstrapped confidence intervals, KDE and QQplot comparisons, and ShapiroWilk tests all supported the conclusion that dwell time distributions are right skewed with dense early activity and long tails, but the low sample size constrains how far these methods can be interpreted.

Manual bucketing proved the most reliable technique for understanding time range patterns, while HDBSCAN clustering offered useful visualizations of tactic-dense periods even if sparse data limited its influence on dwell time derivation.

Overall, the analysis reliably captures behavioural trends but cannot yet support higher resolution modelling without expanded data sets.

Red Team Testing

Detection meta-models were created from the observed intrusions. The Darktrace Red Team is continuously testing the meta-models that were created via threat emulation of Chinese-nexus actors with both success and failure to achieve their goals observed.

Environments were tested against observed adversarial behaviours rather than fixed toolchains. Results showed needed meta model refinement but also have shown promising signs on consistent detection of identity misuse, admin anomalies, and cross-domain pivots, even as tools and infrastructure have changed across suspected Chinese-nexus intrusions.

Appendix 2: References

1. CISA: Tactics, Techniques, and Procedures of Indicted APT 40 Actors
https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-200a

2. FBI CISA Joint Advisory on Compromise of Microsoft Exchange Server
https://www.cisa.gov/news-events/alerts/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server

3. Countering Chinese State Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

4. Sophos: Pacific Rim https://www.sophos.com/en-us/content/pacific-rim

5. International Institute for Strategic Studies: Cyber Capabilities and National Power – China https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---china.pdf

6. PWC: Operation Cloud Hopper https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf

7. National Cyber Security Centre. APT 10 continuing to Target UK organisations https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations

8. US Department of Justice: Press release: Chinese Nationals with Ties to the PRC Government and "APT27" Charged in a Computer Hacking Campaign for Profit, Targeting Numerous U.S. Companies, Institutions, and Municipalities https://www.justice.gov/usao-dc/pr/chinese-nationals-ties-prc-government-and-apt27-charged-computer-hacking-campaign-profit

9. Australian Signals Directorate: Advisory 2020 – 008 Copy-paste compromises - tactics, techniques and procedures used to target multiple Australian networks https://www.cyber.gov.au/about-us/advisories/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks

10. Before Vegas: The "Red Hackers" Who Shaped China's Cyber Ecosystem
https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/before-vegas-cyberdefense-report.pdf

11. World Economic Forum: How China's 15th year five year plan signals a new phase of strategic adaption https://www.weforum.org/stories/2025/10/how-china-s-15th-five-year-plan-signals-a-new-phase-of-strategic-adaptation/

12. Annual Threat Assessment of the U.S. Intelligence Community - https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

13. Asia Society: Memo on U.S. Policy to China https://asiasociety.org/center-us-china-relations/memo-us-policy-china

14. UC San Diego School of Global Policy and Strategy: China's New Five-Year Plan: Strategy, Growth and Its Global Role https://calendar.ucsd.edu/event/chinas-new-five-year-plan-strategy-growth-and-its-global-role

15. The Challenge of Assessing Strategic Cyber Security Risk in Organisations and Critical Infrastructure - https://spp.umd.edu/sites/default/files/2020-09/working-paper-strategic-cyber.pdf

16. FAIR Institute: A FAIR Taxonomy for Cyber Risk Scenarios https://www.fairinstitute.org/hubfs/FAIR%20CRM%20Body%20of%20Knowledge/FAIR%20Institute%20--%20Cyber%20Risk%20Scenario%20Taxonomy%20%28February%202025%29.pdf

17. CISA: 2025 CVE Top 25 Most Dangerous Software Weaknesses https://www.cisa.gov/news-events/alerts/2025/12/11/2025-cwe-top-25-most-dangerous-software-weaknesses

18. Salty Much: Darktrace's view on a recent Salt Typhoon intrusion https://www.darktrace.com/blog/salty-much-darktraces-view-on-a-recent-salt-typhoon-intrusion

19. Library of Congress: Salt Typhoon Hacks of Telecommunication Companies and Federal Response Implications https://www.congress.gov/crs-product/IF12798

20. CISA: PRC State-Sponsor Actors Compromise and Maintain Persistence Access to U.S. Critical Infrastructure https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

21. NCSC Press Release: NCSC and partners issue warning about state-sponsored cyber attackers hiding on critical infrastructure networks https://www.ncsc.gov.uk/news/ncsc-and-partners-issue-warning-about-state-sponsored-cyber-attackers-hiding-on-critical-infrastructure-networks

22. NSA Press Release: ESF Partners, NSA, and CISA Release Identity and Access Management Recommended Best Practices for Administrators
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3336001/esf-partners-nsa-and-cisa-release-identity-and-access-management-recommended-be/

23. US Executive Office of the President: MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES (August 2021) https://whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

24. FCC: FACT SHEET: IMPLICATIONS OF SALT TYPHOON ATTACK AND FCC RESPONSE https://docs.fcc.gov/public/attachments/DOC-408015A1.pdf

25. NCSC, CISA: SAFEGUARDING OUR CRITICAL INFRASTRUCTURE https://www.dni.gov/files/NCSC/documents/products/Final_Safeguarding_Our_Critical_Infrastructure.pdf

26. Fact Sheet: PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders https://media.defense.gov/2024/Mar/19/2003416053/-1/-1/0/FACT-SHEET-FOR-LEADERS-PRC-STATE-SPONSORED-CYBER-ACTIVITY.PDF