New Naval Strategy, Not Cyberwar: China's State-Sponsored Maritime Cyber Operations

Francesco Ferazza and Konstantinos Mersinas
Royal Holloway, University of London, UK

francesco.ferazza@gmail.com
Konstantinos.Mersinas@rhul.ac.uk

Abstract: This paper analyzes state-sponsored cyber operations by the People's Republic of China (PRC) against the global maritime sector from 2015–2025. It moves beyond isolated technical analysis to frame these campaigns as a coherent strategic logic. Using a structured, focused comparison of three PRC-linked intrusion sets—Volt Typhoon, APT40, and Mustang Panda—this analysis assesses their operational characteristics against prominent cyber strategy theories, including capability-intensity barriers, the intelligence-contest logic, and persistent engagement. The findings demonstrate a consistent pattern of behavior across all three cases: operations are capability-intensive, espionage-forward, and prioritize secrecy over overt signaling. This contrasts with other state actors who have used disruptive signaling in the maritime domain. We argue this pattern is explained by Smeets' capability-scarcity logic: high-capability maritime accesses are too costly to expend on peacetime signaling. This behavior aligns with PRC doctrinal concepts of "informationized warfare," which prize system-mapping and pre-positioning. The paper concludes by reframing this activity not as "cyberwar," but as a form of "new naval strategy"—a persistent, below-threshold competition for control over the core components of seapower.

Keywords: Offensive cyber operations, Maritime, Cyber security, Security studies

1. Introduction

Maritime networks are where commerce and seapower meet. The same ports that surge fuel and equipment for military mobility also move the containers on which national economies depend. Between 2015 and 2025, intrusion sets with links to the People's Republic of China (PRC) repeatedly targeted the Transportation Systems sector—including ports and maritime supply chains—using living-off-the-land (LOTL) techniques, edge-device compromises, and long-dwell *pre-positioning* intended to produce options for crisis-time disruption (CISA et al., 2024; CISA, 2024). Interpreting these as isolated attacks underestimates their strategic logic: they fit a pattern of persistent competition below the threshold of armed conflict—*new naval warfare*.

2. Research Question and Scope

RQ: *How, and to what strategic effect, do PRC-linked cyber campaigns operate against the maritime sector (2015–2025), and do their observable characteristics support theories of capability barriers, intelligence contest logics, and persistent engagement within PRC doctrinal concepts of informationized and intelligentized warfare?*

The analysis focuses on three PRC-linked cases with credible open-source coverage of maritime targeting: (i) Volt Typhoon; (ii) APT40/Leviathan (MSS Hainan); and (iii) Mustang Panda (Earth Preta). These cases were selected to provide variation along the capability-intensity dimension while holding constant the actor (PRC nexus) and domain (maritime/transport). Volt Typhoon and APT40 represent high-capability, state-integrated operations; Mustang Panda provides a mid-tier comparator. This "most-similar" design, with Mustang Panda serving as a robustness check on the lower-capability bound, enables testing whether capability maturity conditions the secrecy–signaling trade-off as Smeets predicts (Smeets, 2022).

3. Argument and Contributions

Three claims are advanced. First, offensive cyber against maritime targets is *capability intensive* (Smeets), reflected in bespoke tooling, edge-device exploitation, and organizational integration (Smeets, 2022). Second, observed campaigns are *espionage-forward* (Lindsay), prioritizing secrecy, mapping, and option-setting over overt coercion (Lindsay, 2013, 2015). Third, the *operational cadence* is shaped by *persistent engagement* (Harknett, Goldman, Fischerkeller), featuring continuous contact, pre-positioning, and iterative re-entry below the use-of-force threshold (Fischerkeller et al., 2022; Harknett and Smeets, 2022).

These are situated within PRC doctrinal concepts of *informationized* and *intelligentized* warfare (State Council Information Office, 2015; U.S. Department of Defense, 2023) and informed by maritime cyber scholarship that articulates strategic logics for the domain (Ferazza and Mersinas, 2025). Substantively, the paper provides a PRC-focused account of maritime cyber behavior. Theoretically, it integrates Smeets–Lindsay–Harknett into a testable scaffolding with observable implications and explicit trade-offs between signaling and secrecy.

4. Doctrinal Background: Strategic Logics of Offensive Cyber Operations

Here we lay out three practical ways to make sense of offensive cyber operations in the maritime world. Our framing tracks recent maritime work and builds on the broader cyber strategy literature (Rid, 2013; Valeriano and Maness, 2015). The goal is to provide a map for thinking about what these campaigns try to achieve and how they go about it. Figure 1 illustrates and summarizes these three logics.

4.1 Offensive Cyber Operations with Disruptive Effects

Offensive cyber operations with disruptive effects degrade or disrupt adversary capabilities through overt technical actions. Following Smeets (Smeets, 2022), such operations generate strategic value through multiple mechanisms: as force multipliers in conventional operations, as independent instruments of friction, or—when deliberately visible—as coercive signals that demonstrate capability and resolve.When used for coercive purposes, these operations function as forceful signals, compelling behavioral change through visible punishment rather than clandestine access. The strategic trade-off is fundamental: visibility enables signaling and psychological effects but necessarily sacrifices the long-term clandestine access that intelligence operations require. In dual-use maritime systems, visible disruptions—such as port terminal outages or GPS spoofing—can achieve coercive effects while remaining below the threshold of armed conflict.

Linking capability to signaling (Smeets). Smeets' account of organizational and technical barriers implies that *accesses and bespoke capabilities are scarce assets*; burning them for overt signaling is costly (Smeets, 2022). Where PETIO capacities (People, Exploits/tools, Targets, Infrastructure, Organization) are *thin*, operators face stronger incentives to preserve secrecy and dwell; where PETIO is *thick* and replenishable, calibrated signaling becomes more feasible. This predictable asymmetry helps explain the observed bias toward intelligence-first activity in capability-intensive maritime targets.

4.2 Intelligence Contest

The intelligence-contest logic prioritizes clandestine collection, network mapping, and *pre-positioning* of accesses. Value derives from secrecy and dwell time, with latent options for disruption should crisis conditions warrant (Lindsay, 2013; Rovner, 2019). In maritime networks, targeted data may include cargo manifests, vessel schedules, port control software (Terminal Operating Systems, TOS), engineering documentation, and vendor access pathways. The secrecy–signaling dilemma is central: publicity and disruption can forfeit long-run intelligence advantage (Rid and Buchanan, 2015).

4.3 Persistent Engagement

Persistent engagement describes the structural condition of continuous contact, where actors compete for initiative through ongoing campaigns below the use-of-force threshold (Fischerkeller et al., 2022). Rather than discrete "wars," the maritime domain experiences cumulative shaping: iterative probing, pre-positioning, and rapid re-entry post-eviction. Maritime research explicitly nests signaling, cost-imposition, coercion, and intelligence contests within this persistent environment (Ferazza and Mersinas, 2025).

4.4 PRC Doctrinal Integration of OCO Logics

PRC doctrinal materials emphasize winning "informationized local wars" and achieving informa-tion dominance via system-of-systems paralysis (State Council Information Office, 2015; U.S. Department of Defense, 2023). These concepts align theoretically with both the intelligence con-test (mapping enemy systems for information advantage) and persistent engagement (continuous below-threshold competition).

Recent analyses describe a doctrinal shift toward *intelligentized* warfare—the integration of artificial intelligence into sensing, decision-making, and operational effects (CNA, 2021; Kania, 2019). This evolution potentially lowers the capability costs (PETIO barriers) that Smeets identifies, making previously expensive accesses more renewable. However, no explicit evidence of AI integration in the observed campaigns has been reported; therefore, for the purposes of this empirical analysis, intelligentized warfare is treated as a doctrinal intent for future capability rather than a demonstrated current-state operational capability.

Targeting of ports and shipping aligns with these concepts and with longstanding seapower concepts (Mahanian commercial interdiction; Corbettian sea control/denial) adapted to the cyber domain. The cyber domain is inherently naval when it targets the physical and information systems of *seapower* : the ports, vessels, and supply chains that constitute the operational base for economic and military mobility (Till, 2013; Holmes and Yoshihara, 2010).

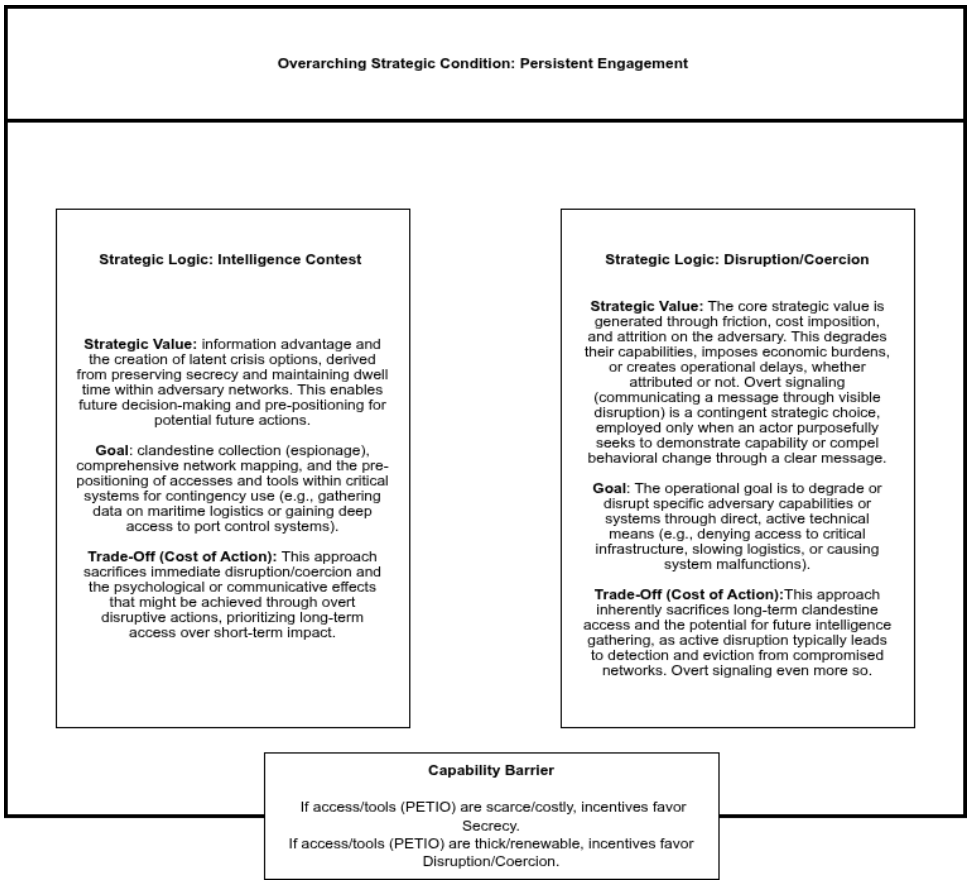

Figure 1: A diagram illustrating and summarizing the OCOs strategic logics (Intelligence Contest vs. Disruption/Coercion within Persistent Engagement)

5. Methodology

5.1 Design and Scope

We use a small set of well-documented cases and read them closely. The design is a structured, focused comparison paired with process tracing. In practice, that means we ask the same questions of each case (who/how/why) and then look inside the timeline for clues that link causes to outcomes. This follows standard comparative case-study practice and the process-tracing playbook (George and Bennett, 2005; Gerring, 2017). We are not trying to estimate population-wide effects; the aim is to sharpen theory with carefully chosen evidence.

5.2 Case Selection and Attribution

We utilize a classic "most-similar" strategy: we pick cases that vary on capability but hold the ac-tor (PRC nexus) and domain (maritime/transport) roughly constant. Selection is constrained by credible public detail. The three cases that meet these bars are Volt Typhoon, APT40/Leviathan, and Mustang Panda. These anchor a comparison of high-capability, state-integrated operations (Volt Typhoon, APT40) against a mid-tier cluster (Mustang Panda), the latter serving as a robustness check.

We express attribution in plain probabilistic terms (e.g., "moderate confidence"), leaning on joint US/allied advisories, official statements, and convergent vendor work. This mirrors best practice in the cyber attribution literature and helps avoid over-claiming (Rid and Buchanan, 2015).

5.3 Analytical Heuristic and Coding

To compare across cases, we score a handful of dimensions (D1–D7) with short, ordinal scales.

- **D1 (Capability intensity):** Signs of bespoke tooling, edge-device or zero-day use, distributed C2, and organizational integration. Scale: 0–2 (Smeets, 2022).

- **D2 (Pre-positioning):** Long dwell, LOTL, router/SOHO footholds, explicit crisis-activation language. Scale: 0–2 (Fischerkeller et al., 2022).
- **D3 (Intelligence-first):** Collection and mapping dominate; disruption is latent. Scale: 0–2 (Lindsay, 2015).
- **D4 (Doctrine fit):** Alignment with PRC "system-paralysis" and information dominance concepts. Scale: 0–2 (State Council Information Office, 2015).
- **D5 (Target logic):** Counterforce (military enabling) versus countervalue (commer-cial/economic). Scale: 0 (Pure Commercial) to 2 (Pure Military).
- **D6 (Secrecy vs. signaling):** Qualitative coding (Secrecy / Mixed / Signaling).
- **D7 (Environment dependence):** Evidence of iterative probing and re-entry. Ordinal: Absent / Partial / Present.

Process Tracing. We use standard process-tracing tests to assess whether evidence meaning-fully links cause and effect (Van Evera, 1997). Following Van Evera's typology: a *smoking gun* (e.g., advisory language explicitly mentioning crisis-time disruption) is strong but not required; a *hoop test* (e.g., distributed C2 indicating capability intensity) must be passed but is not sufficient on its own; *straws in the wind* (e.g., USB propagation into OT) are suggestive but weak. We look for multiple, independent pieces that point the same way to guard against cherry-picking.

6. Analysis of the Cases

6.1 Volt Typhoon (PRC): Pre-positioning in U.S. Critical Infrastructure

Who and How. Multi-agency U.S. and partner advisories assess (High Confidence) that PRC state-sponsored actors are maintaining persistent, stealthy access across critical infrastructure, including the Transportation Systems sector (CISA et al., 2024). Their tradecraft involves credential harvesting, valid account abuse, and extensive use of compromised SOHO routers as covert C2. This reliance on living-off-the-land (LOTL) binaries and disciplined OPSEC allows them to avoid detection while maintaining long-term access (U.S. DOJ, 2024).

Why and Strategic Logic. The assessed objective is to enable *crisis-time disruption* and impose operational friction, with particular concern for Guam-adjacent and CONUS nodes relevant to Indo-Pacific logistics. Within the strategic-logics frame, behavior aligns primarily with the *intelligence contest* nested in *persistent engagement* : access is preserved, mapping is extensive, and signaling is limited.

Process Tracing. The CISA advisory language explicitly stating "crisis-time disruption" pathways constitutes a **smoking-gun test** for D2 (pre-positioning). The distributed SOHO router C2 infrastructure serves as a **hoop test** for D1 (capability intensity), indicating the significant infrastructural investment required.

Coding Summary: D1=2 (High Capability); D2=2 (High Pre-positioning); D3=2 (Intel-First); D4=2 (Doctrine Fit); D5=1 (Dual-Use); D6=Secrecy-dominant; D7=Present.

6.2 APT40 / Leviathan (MSS Hainan): Maritime Espionage at Scale

Who and How. APT40 (Leviathan) is widely associated with MSS Hainan (High Confidence) (FBI and CISA, 2021). Historic reporting emphasizes a multi-year focus on maritime engineering and shipping. Their methods include spearphishing, web server exploitation, and the use of *custom backdoors* and waterholing. The operational behavior indicates integrated tasking and persistent collection of engineering and logistics data (MITRE ATT&CK, 2025).

Why and Strategic Logic. Primary objectives are *collection and mapping* for intelligence

advantage and contingency options. Visibility tends to coincide with law-enforcement or diplomatic actions (e.g., 2021 indictments) rather than deliberate signaling by the operators (UK FCDO, 2021).

Process Tracing. The use of custom backdoors constitutes a **smoking-gun test** for D1 (bespoke tooling). Multi-year sustained access serves as a **hoop test** for D2 (pre-positioning).

Coding Summary: D1=2; D2=2; D3=2; D4=2; D5=1 (Dual-Use); D6=Secrecy-dominant;

D7=Present.

6.3 Mustang Panda (Earth Preta): European Shipping Firms

Who and How. The PRC-linked cluster Mustang Panda (Earth Preta) has been observed tar-geting European shipping companies with Moderate Confidence (The Maritime Executive, 2024). Their tradecraft relies on Korplug/PlugX loaders (known tooling with moderate customization) and removable-media (USB) propagation. In certain cases, initial droppers appear to have been launched from a USB drive, with some infections observed aboard vessels (CyberOwl, 2024).

Why and Strategic Logic. The aim appears to be intelligence-first: data collection, network mapping, and potential contingency access. However, tool reuse and mid-tier infrastructure indicate comparatively lower capability intensity than APT40 or Volt Typhoon.

Process Tracing. USB propagation into onboard systems serves as a **straw-in-the-wind test** for D2 (pre-positioning in hard-to-reach operational technology environments).

Coding Summary: D1=1 (Mid Capability); D2=1 (Episodic Pre-positioning); D3=2; D4=1; D5=0 (Pure Countervalue); D6=Secrecy-dominant; D7=Partial.

6.4 Comparative Context: PRC vs. Other State Actors

To contextualize PRC behavior, we briefly compare against non-PRC maritime cases. Russia's NotPetya attack (2017) on Ukraine achieved massive disruptive effects globally, crippling Maersk's shipping operations (Greenberg, 2018). If coded on our scheme, NotPetya would score as a high-capability tool (D1=2) but purely destructive (D3=0) and a clear coercive signal (D6=Signaling). Similarly, Iran's disruption at Shahid Rajaee Port (2020) was a visible retaliatory signal.

In contrast, all three PRC cases examined here prioritize secrecy, long dwell, and collection over visible disruption. This pattern suggests that PRC maritime cyber strategy reflects a distinct calculus: high capability costs and organizational investment in maritime-specific accesses create strong incentives to preserve those accesses for long-term intelligence advantage, rather than expending them on peacetime signaling.

7. Discussion of the Analysis

The cases exhibit strong, convergent support for D1–D3. Volt Typhoon and APT40 display mature PETIO stacks—bespoke implants or infrastructure, edge-device tradecraft, distributed C2, and disciplined OPSEC. In both, pre-positioning and long dwell are endemic, with ex-plicit language in advisories regarding crisis-time disruption pathways. Mustang Panda shows intelligence-first priorities with mid-tier capability indicators.

Strategic Logics. The intelligence-contest logic dominates (collection, mapping, option-setting), with disruptive signaling comparatively rare. This secrecy–signaling dilemma is consistent with Lindsay's intelligence-contest framework and with cumulative competition under persistent engagement (Lindsay, 2015).

Doctrine Fit and Targeting. The victim sets—ports, shipping, logistics/communications nodes—align with PRC concepts of informationized warfare and with the targeting aims of intelligentized warfare (D4). Dual-use infrastructures blur counterforce/countervalue distinctions (D5=1), increasing escalation ambiguity. Volt Typhoon's targeting of transportation/maritime nodes critical to Indo-Pacific military mobility exemplifies this dual-use challenge: the same port that handles commercial cargo also serves as a military logistics node.

Capability and Signaling (Smeets Revisited). The observed restraint in visible disruption is consistent with Smeets' logic: when accesses and bespoke tools are costly to generate and maintain, organizations prefer to "bank" them for future leverage rather than expend them on one-off signals. Volt Typhoon's distributed SOHO router infrastructure represents significant infrastructural investment (I in PETIO); APT40's custom backdoors indicate mature People and Exploits (P, E) (Smeets, 2022).

Escalation Dynamics and Thresholds. All three cases operate demonstrably below the threshold of armed conflict. The operations avoid kinetic effects, casualties, or immediate physical damage. However, the pre-positioning for crisis-time disruption creates latent escalation pathways. The threshold calibration appears deliberate: maintain access and options while avoiding actions that would compel a military response or cross legal red lines established in frameworks like the Tallinn Manual 2.0 (Schmitt, 2017).

8. Limitations and Future Research

We try to be clear about what could trip us up. Open-source attributions can be contested; we largely rely on primary advisories to mitigate this. Western visibility may bias incident samples toward operations against allied networks. Furthermore, the reliance on non-primary sources for Mustang Panda is a case-selection constraint.

Future research should focus on: building panel datasets linking port operational metrics to campaign timelines; quantifying re-entry rates post-eviction; measuring "option depth" (distinct activation paths); and studying AI-enabled elements of intelligentized campaigns. Additionally, exploring legal/normative implications for maritime cyber thresholds remains a priority.

9. Conclusions

PRC maritime cyber campaigns in 2015–2025 exhibit capability intensity, pre-positioning, and an intelligence-first orientation executed within a persistent-engagement environment. Targeting coheres with PRC doctrines of informationized and intelligentized warfare and exploits the dual-use nature of maritime infrastructure. The comparative analysis reveals a distinctive PRC approach: unlike Russian operations that have employed visible disruption for coercive signalling, PRC maritime campaigns prioritise access preservation, long dwell, and mapping. This aligns with capability-scarcity logic: valuable accesses are too costly to expend on peacetime signalling. The evidence supports reframing this activity as new naval strategy—persistent, below-threshold competition for control over the information systems constituting seapower. Whether such competition constitutes a new form of naval warfare depends on definitional commitments this paper cannot resolve. Under Clausewitzian criteria requiring violence and political attribution, these operations fall short; under persistent-engagement frameworks that reject the war/peace binary, they may represent naval conflict conducted entirely below the threshold of armed force. What the evidence does establish is that these campaigns follow coherent maritime-strategic logic—not generic "cyberwarfare"—and demand recognition as sustained competition in the naval domain. Policies prioritising rapid detection to deny dwell, identity and access management controls to break LOTL exploitation, and router hygiene offer pathways to raising attacker costs without precipitating escalation. Policy must recognise the persistent nature of the threat and emphasise continuous adaptation over one-time solutions.

Ethics declaration: Ethical clearance was not required for this research.

AI declaration: AI was used to solve Latex `formatting` issues, and for grammar and sentence-flow checking on Overleaf.

References

Alexander L. George and Andrew Bennett, Case Studies and Theory Development in the Social Sciences. MIT Press, 2005.
Alfred Thayer Mahan, The Influence of Sea Power upon History, 1890.
Andrew Bennett and Jeffrey T. Checkel (eds.), Process Tracing. Cambridge University Press, 2014.
Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, Aug. 22, 2018.
Ben Buchanan, The Hacker and the State. Harvard University Press, 2020.
Brandon Valeriano and Ryan C. Maness, Cyber War versus Cyber Realities. Oxford University Press, 2015.
CISA, "Fact Sheet: PRC Linked 'Volt Typhoon' Activity," Mar. 19, 2024.
CISA, FBI, NSA, et al., "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Joint Cybersecurity Advisory AA24-038A, Feb. 7, 2024.
CNA Corporation, "The PLA and Intelligent Warfare: A Preliminary Analysis," Oct. 2021.
CyberOwl, "Responding to news on malware on Greek, Dutch and Norwegian ships," May 21, 2024.
Derek Beach and Rasmus Brun Pedersen, Process-Tracing Methods. 2nd ed., University of Michigan Press, 2019.
Elsa B. Kania, "AI Weapons in China's Military Innovation," Brookings Institution, 2020.
FBI & CISA, "APT40 Targeting: Tactics, Techniques and Procedures of Indicted Actors Associated with China's MSS Hainan State Security Department," Joint Advisory AA21-200A, July 19, 2021.
FireEye Threat Intelligence, "APT40: Examining a China-Nexus Espionage Actor (TEMP.Periscope)," Mar. 4, 2019.
Francesco Ferazza and Konstantinos Mersinas, "Non-Kinetic Naval Strategy: The Role of Cyber Operations in Modern Maritime Conflict." Journal of Cybersecurity, 2025. doi:10.1093/cybsec/tyaf031.
Geoffrey Till, Seapower: A Guide for the Twenty-First Century, 3rd ed., Routledge, 2013.
James R. Holmes and Toshi Yoshihara, Red Star Over the Pacific, Naval Institute Press, 2010.
Jason Seawright and John Gerring, "Case Selection Techniques," Political Research Quarterly 61(2), 2008.
John Gerring, Case Study Research: Principles and Practices. 2nd ed., Cambridge University Press, 2017.
Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," Security Studies 22(3), 2013.
Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," International Security 39(3), 2015.
Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," International Security 41(3), 2017.

Joshua Rovner, "Cyber War as an Intelligence Contest," War on the Rocks, Sept. 16, 2019.
Max Smeets, No Shortcuts: Why States Struggle to Develop a Military Cyber-Force. Oxford University Press, 2022.
Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.
Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, Cyber Persistence Theory. Oxford University Press, 2022.
MITRE ATT&CK, "Leviathan, Group G0065 (APT40, TEMP.Periscope)," accessed Oct. 2025.
Richard J. Harknett and Max Smeets, "Cyber campaigns and strategic outcomes," Journal of Strategic Studies 45(4), 2022.
Robert K. Yin, Case Study Research and Applications. 6th ed., SAGE, 2018.
State Council Information Office (PRC), "China's Military Strategy," May 2015.
Stephen Van Evera, Guide to Methods for Students of Political Science. Cornell University Press, 1997.
The Maritime Executive, "Chinese Spy Malware Found in European Shipping Companies' Systems," May 15, 2024.
Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," Journal of Strategic Studies 38(1–2), 2015.
Thomas Rid, Cyber War Will Not Take Place. Hurst/Oxford University Press, 2013.
Transportation Security Administration (TSA), "TSA Issues Cybersecurity Advisory on PRC State-Sponsored Activity," Press Release, Feb. 7, 2024.
U.S. Department of Defense, Military and Security Developments Involving the People's Republic of China 2023, Oct. 2023.
U.S. Department of Justice, "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure" Press Release, Jan. 31, 2024.
UK Foreign, Commonwealth & Development Office, "UK and allies hold Chinese state responsible for a pervasive pattern of hacking," July 19, 2021.

Appendix A: Per-Case Scoring (D1–D7)

Case Dim Score & Justification

Volt Ty-phoon

- D1 **2** — Distributed C2 via compromised SOHO routers; disciplined OPSEC; multi-agency integration.
- D2 **2** — Advisory language explicitly references "crisis-time disrup-tion"; LOTL and router footholds enable long-dwell
- D3 **2** — Collection/mapping dominate; minimal overt effects re-ported.
- D4 **2** — Targeting of transportation nodes critical to Indo-Pacific military logistics aligns with system-paralysis aims.
- D5 **1** — Dual-Use assets (civilian infra with military logistics role).
- D6 **Secrecy** — Long undetected dwell; disclosed via defender investigation.
- D7 **Present** — Evidence of iterative probing campaigns.

APT40

- D1 **2** — Custom backdoors; sustained sectoral focus; web server exploitation.
- D2 **2** — Years-long sustained activity with durable pre-positioning.
- D3 **2** — Espionage-first: collection of engineering/logistics data dominates.
- D4 **2** — Enables comprehensive mappingof adversary naval/commercial maritime systems.
- D5 **1** — Dual-Use (commercial entities but military-relevant data). D6 **Secrecy** — Visibility from law-enforcement actions, not opera-tor intent.
- D7 **Present** — Recurrent campaigns across multiple years.

Mustang Panda

- D1 **1** — Known tools (PlugX) with moderate customization; USB propagation.
- D2 **1** — USB-based footholds suggest persistence, but lack multi-year evidence of Volt Typhoon.
- D3 **2** — Collection and network mapping are primary aims.
- D4 **1** — Targeting commercial shipping provides economic intelli-gence; indirect strategic alignment.
- D5 **0** — Pure Countervalue (commercial shipping). D6 **Secrecy** — Disclosed via vendor reporting.
- D7 **Partial** — Recurrence in European shipping sector but less systematic.