Booz Allen®

Breaking Through:

How to Predict, Prevent, and Prevail over the PRC Cyber Threat

Approved for Public Release. September 2025.

Table of Contents

Executive Summary

1

Executive Summary

The People's Republic of China (PRC)[a] conducts cyber operations that are strategic, persistent, and global. From breaching government agencies and prepositioning in ports, to deploying ransomware for political coercion and honing influence operations with AI, these operations are well documented. But their cumulative strategic impact remains poorly understood and insufficiently integrated into U.S. planning. These operations constrain U.S. options in future crises and geostrategic competition. Overcoming this challenge requires understanding the technical accelerants of PRC cyber power, the global systemic conditions it exploits, and the national actions needed to push back against these encroaching constraints. This report provides that insight.

This report analyzes the defining methods, global patterns, and strategic logic behind PRC cyber operations. It offers a structured assessment of how Beijing uses cyber power as an instrument of coercion, to erode resilience, fracture alliance coordination, and limit the ability of the U.S. and its partners to act decisively. By linking operational techniques, such as edge device exploitation, vendor-enabled access, and AI-scaling, to specific regional campaigns, the report shows how previously siloed incidents reflect a coherent strategy to reshape the terms of global competition.

Again and again, PRC cyber operations have reportedly caught the U.S. and its allies and partners by surprise.[3] [4] The U.S. must break this cycle. National leaders must not assume any sectors are secure or underestimate the PRC's capacity to deliberately evolve its tradecraft in pursuit of strategic goals. Future policy must anticipate the PRC's growing scale, speed, and agility, not just replicate past breach playbooks. This report is designed to inform that shift by offering insight into how PRC cyber operations are likely to expand, adapt, and entrench over the next five years.

Reversing these trends will require urgent national action coordinated with international allies and partners to expose, contest, and dislodge PRC footholds before they harden into structural disadvantages for the United States. The recommendations that follow span cyber defense modernization, vendor access reform, attribution posture, and strategic engagement. Each is designed to help cyber leaders move from reactive defense to proactive shaping—rebuilding resilience, restoring initiative, and preserving decision-making advantage. The window to act is narrowing, but with deliberate strategy and sustained investment, the U.S. can blunt Beijing's advances, reclaim operational advantage, and reset the terms of long-term competition.

[a] In this report, "**People's Republic of China**" refers to the sovereign state commonly known as "China," in alignment with U.S. policy since the 1970s. The term "Chinese" is used in an ethnic or cultural context unless explicitly linked to the state or its official entities.

Key Findings

2

Key Findings

- Beijing is building a cyber-enabled positional advantage that systematically erodes U.S. strategic initiative across time, terrain, and tempo. These changes may fundamentally constrain how the U.S. can coordinate, respond, and compete.
- Beijing's cyber strategy leverages four force-multipliers—trusted-relationship compromise, edge device exploitation, AI acceleration, and attribution contestation—maximizing operational reach, stealth, speed, and deniability.
- Trusted-relationship abuse is giving the PRC strategic advantage by establishing persistent access that bypasses conventional cyber defenses and erodes U.S. response capabilities.
- PRC dominance in network edge exploitation creates systematic access advantages that degrade U.S. situational awareness and outpace decision cycles.
- AI accelerates PRC cyber operations by enabling speed and precision across reconnaissance, exploit and malware development, targeting, and data processing.
- PRC actors are using AI to overcome structural barriers that have long constrained Beijing's influence in foreign information environments.
- The PRC's shift from denying to contesting attribution risks fragmenting allied responses and preserving PRC freedom to operate below escalation thresholds.
- PRC cyber operations aim to constrain U.S. power in three strategic arenas by eroding agility and escalation control in East Asia, fracturing alliance coordination in Europe and the Five Eyes, and embedding economic and geopolitical leverage across the developing world.
- Without deliberate national action, the PRC's cyber and influence gains may harden into structural advantages, potentially reshaping the global operating environment in its favor.

Counter-Strategy at a Glance

3

Counter-Strategy at a Glance

Objective	Core Moves	What it Buys the U.S.
Close the Trusted Back Door	Treat all third-party sessions as hostile until proven otherwise; log, segment, broker, and red-team vendor access.	Halts the PRC's scalable access via update and support channels.
Fortify the Edge	Harden firewalls, VPNs, satellite/cellular gateways and operational technology (OT) firmware; bring edge devices into visibility and hunt cycles.	Removes the PRC's favored footholds for access.
Build and Buy Secure	Bake "adversarial control risk" into every hardware and software purchase. Use purchasing power to incentivize security by design.	Starves the PRC of access via supply chain compromise.
Burn the Botnet and Relay Layer	Track, indict, and dismantle contractor-run infrastructure-as-a-service, not just front-line threat actors.	Cuts operational reach, deny stealth, and impose cost.
Out-Automate and Undermine the Adversary	Deploy mission-focused AI for triage, anomaly detection, and influence-ops tracking. Develop and apply counter-AI techniques to disrupt PRC model performance.	Hollows out the PRC's offensive automation advantage.
Fight the Attribution Fight	Create declassification pathways and joint government-industry messaging to go public with fast and unassailable attribution.	Burns the PRC denial playbook and sustain allies' and partners' consensus over attribution.
Break the Influence Chain	Track narrative flows, dismantle amplification infrastructure, expose influence networks, and disrupt the digital supply chain of PRC information warfare online.	Forces covert PRC influence operations out of the shadows and off the board.
Forward-Posture with Partners	Deploy hunt teams, harden frontline systems, and integrate regional allies and partners into joint response planning.	Denies Beijing uncontested terrain, preserve coalition cohesion, and protect strategic access before crises erupt.
Draw Allies Closer	Harden shared supply chains, empower allies to expose PRC operations, and defend crisis-response infrastructure.	Blunts PRC efforts to fracture coalitions and accelerate joint response.
Deny Digital Entrenchment	Displace PRC technology, embed partner-facing teams, and build regional cyber readiness.	Dislodges PRC footholds, secure critical terrain, and preserve U.S. access.

Introduction

4

Introduction

The PRC has built a cyber operations ecosystem optimized for scale, persistence, and strategic effect. Its cyber campaigns are more than a collection of intrusions to expel and remediate. They are a tool of statecraft, applied systematically with other elements of national power to weaken adversaries' decision-making ecosystems, constrain their operational flexibility, and pre-condition the outcomes of future geopolitical contests. What distinguishes the PRC's cyber offense today is more than the breadth of its targeting or the persistence of its access: It is Beijing's fusion of national strategy, technical innovation, and exploitation of global systemic circumstances into a disciplined architecture of geopolitical cyber power.

Much has already been written about discrete aspects of this challenge, like technically novel PRC-attributed campaigns, its contractor and zero-day ecosystems, and targeting trends. But for senior decision-makers, what is often missing is an organizing logic: a way to see how these campaigns accumulate across regions, how tradecraft aligns with strategic outcomes, and how structural conditions—legal, technical, and economic—are enabling a long-term erosion of U.S. strategic freedom. This report is designed for readers who already understand the scale of the threat. It offers them a structured analysis to understand how the PRC uses cyber operations not only to collect intelligence or prepare battlespaces, but to shape the geopolitical environment itself.

The analysis draws on a review of over 350 public reports from the past two and a half years. From this, it identifies four force multipliers that define the PRC's approach to cyber power projection: (1) scaling access with trusted relationships, (2) growing persistence and speed through network edge device exploitation, (3) accelerating operational tempo with AI, and (4) preserving escalation control by contesting attribution. The report then maps how Beijing deploys these capabilities to outmaneuver, weaken, and constrain the US across East Asia, its core alliances, and the developing world. From data leaks in the Pacific Islands to political espionage in Europe and telecom exploitation in South America, the report draws through-lines across what might otherwise appear as unrelated events. It shows how these methods support Beijing's efforts to degrade resilience, fracture shared operational posture, and narrow the window for decisive U.S. action.

This report explains how Beijing is methodically shifting the balance of initiative in cyberspace and what that means for U.S. power. Rather than merely catalog intrusions, it reveals the strategy behind them: the operational logic, enabling conditions, and cumulative effects that threaten to restructure the global operating environment. Leaders tasked with safeguarding national resilience and preserving freedom of action must understand these dynamics to craft an effective response that moves beyond reactive triage and toward sustained strategic advantage. Inaction compounds risk. The U.S. must act urgently to expose, contest, and dislodge PRC advantages before they harden into structural dominance.

The PRC's Approach to Cyber Projection

Scaling access with trusted relationships

Growing persistence and speed through network edge device exploitation

Accelerating operational tempo with AI

Preserving escalation control by contesting attribution

Threat Landscape

5

Threat Landscape

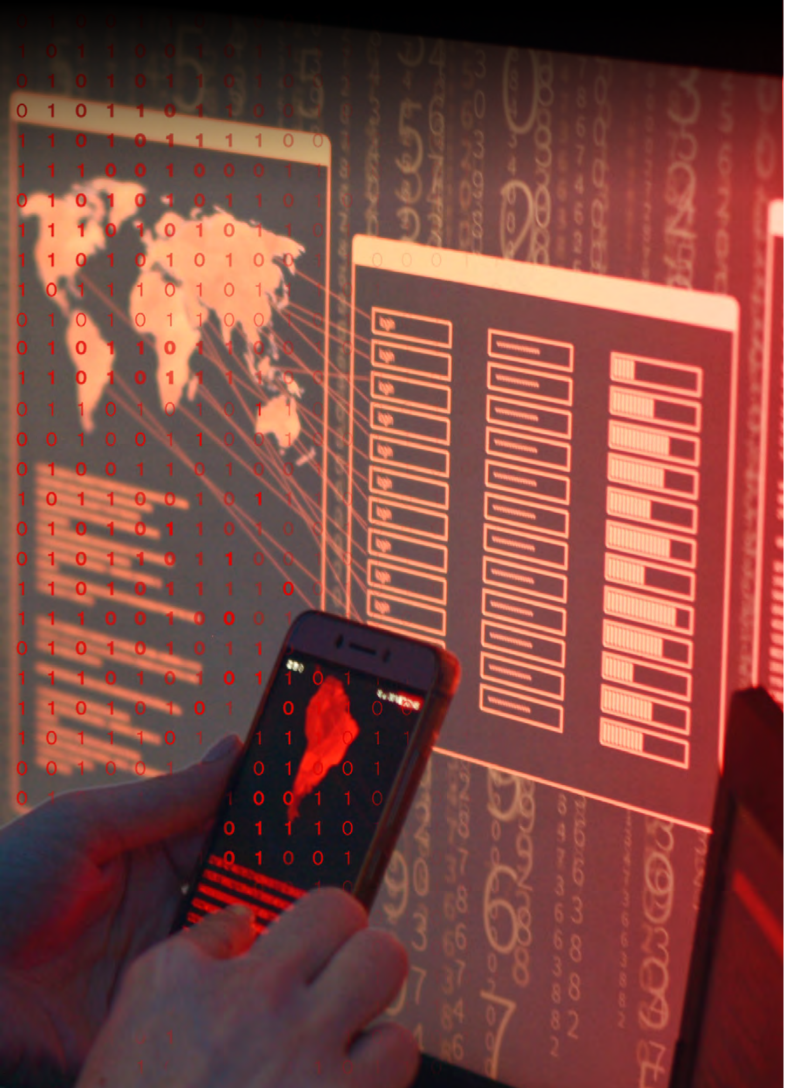
The current PRC cyber threat landscape can be understood through two intersecting lenses: force multipliers that are growing Beijing's cyber power, and the regional arenas where its capabilities are strategically applied. The first half of this section identifies four force-multipliers that indicate Beijing's approach to cyber power projection. These emphasize scale, stealth, speed, and deniability. The second half examines how these methods are applied in three key arenas: the PRC's eastern strategic periphery, the U.S. alliance system, and the developing world. Together, this approach reflects a coherent national effort by the PRC to effectively erode its opponents' cohesion, shape geopolitical alignment, and maneuver crises under the threshold of open conflict.

Force Multipliers

Trusted Relationships Scale Access

Beijing is weaponizing trusted relationships. Rather than breach hardened systems head-on, PRC operators compromise the trusted connections underlying digital infrastructure: between vendors and clients, software platforms and users, administrators and their networks, developers and their supply chains. These pathways provide legitimate access with minimal scrutiny and deep system integration. By embedding themselves into these relationships—whether through stolen credentials, hijacked update channels, or vendor compromise—PRC actors gain scalable, persistent access that bypasses traditional defenses. This creates a fundamental advantage: extended presence with reduced detection risk, lower operational costs, and undermined assumptions in cyber defense frameworks.

This exploitation of trust shifts the burden of defense onto the U.S. and its allies, forcing costly changes to how vendor access, update mechanisms, and administrative privileges are managed. Measures like deeper vendor vetting, segmentation of support tooling, and integrity validation of software delivery pipelines require time, resources, and architectural change. They often degrade operational efficiency in the process. These costs fall especially hard on sectors with legacy infrastructure or deep vendor entanglement, such as operational technology (OT)-heavy critical infrastructure and state and local governments, where modernization timelines are slow and trusted pathways are often exceptions to segmentation. As PRC operators scale access through others' infrastructure, defenders are left absorbing asymmetric costs and friction that compound over time, especially during crisis response or time-sensitive operations.



Vendor Access as a Point of Entry

Vendor-enabled access remains a critical enabler for PRC cyber operators seeking durable, low-friction entry into hardened networks. Rather than relying exclusively on phishing or exploit-based intrusion, PRC-linked actors have increasingly abused trusted relationships between service providers and their clients. These intrusions often exploit VPN credentials, remote support tools, or compromised software updates, allowing access through authorized, allowlisted channels. This model is particularly effective in sectors where vendor connections are managed exceptions to otherwise strict segmentation, such as government and OT-reliant sectors—which includes 13 of 16 designated U.S. critical infrastructure sectors.[5]

- In 2018–2019, **Mustang Panda** and **BlackTech** used stolen VPN credentials from Taiwanese IT vendors to compromise government systems.[6][7][8]
- In late 2024, **Silk Typhoon** exploited two zero-day vulnerabilities in BeyondTrust's Remote Support software and obtained an API key used to reset credentials for cloud-based customer environments. The intrusion enabled access to multiple government networks, including the U.S. Treasury Department's Office of Foreign Assets Control, through a federal support contractor. During the same period and into early 2025, the group applied similar tactics to target U.S. state and local governments, as well as the IT sector, and obtain data concerning law enforcement investigations and other government policy relevant to PRC interests.[9]

PRC operators increasingly treat vendor access as a scalable intrusion vector for multi-target operations across shared ecosystems. This approach reflects a shift toward establishing presence inside vendor environments to enable broader client access. Cloud-based infrastructure and centralized administration have expanded the reach and efficiency of this model, allowing PRC actors to conduct scalable campaigns while minimizing exposure and resource expenditure.

- Between June 2024 and January 2025, PRC-linked operators exploited a vulnerability in Check Point VPN software to steal credentials and access manufacturing organizations across Europe, Africa, and the Americas. The ShadowPad remote access tool was widely deployed, and ransomware was delivered in a limited number of cases.[10]
- In mid-2024, PRC-linked operators targeted large B2B IT service providers in Southern Europe in a campaign dubbed **Operation Digital Eye**, likely aiming to use vendor environments to pivot to access downstream client networks.[11]
- In 2024, the PRC-linked cluster **PurpleHaze** targeted a third-party logistics vendor previously responsible for provisioning employee hardware at a U.S. cybersecurity company.[12] The intrusion, which used the ShadowPad malware, appeared intended to establish indirect access to client environments by exploiting residual trust in the vendor relationship.

Compromise of Software Delivery Channels

PRC software supply chain compromises have evolved from broad deployment with post-compromise filtering to selective delivery at the point of infection. Early campaigns cast a wide net, embedding backdoors in widely distributed software but activating second-stage payloads only on select systems. Over time, operators moved from automated filtering within malware to human-driven triage, and eventually to pre-compromise targeting. This evolution reduces risk, increases operational control, and reflects a growing emphasis on stealth and precision in PRC cyber tradecraft.

- In 2017 and 2018, campaigns that abused updates for CCleaner and ASUS computers to deploy ShadowHammer malware relied on mass software distribution, but embedded filtering logic into the malware itself to limit activation. CCleaner was installed on over 2 million systems, yet only a few dozen triggered second-stage payloads.[13] ShadowHammer updates were pushed broadly but executed only on devices with specific MAC addresses hardcoded into the installer.[14] [15] [16]

- In the 2017 NetSarang incident, **APT41** inserted the ShadowPad backdoor into signed updates for IT administration tools, resulting in widespread compromise.[17] Instead of embedding filters in the malware, operators conducted post-access reconnaissance and delivered second-stage payloads only to a subset of infected systems (primarily in finance, pharmaceutical, and software sectors) reflecting human-driven victim selection after compromise.

- By 2021, PRC operators increasingly limited malware delivery to pre-selected targets. **Tick** compromised a South Korean DLP vendor and used its update channel to infect only a few downstream clients.[18] [19] In 2023, an investigation into 2,000 installations of Cobra DocGuard found that **Carderbee** delivered trojanized updates to only about 100 systems primarily in Hong Kong, suggesting that delivery was scoped to preselected victims prior to deployment.[20]

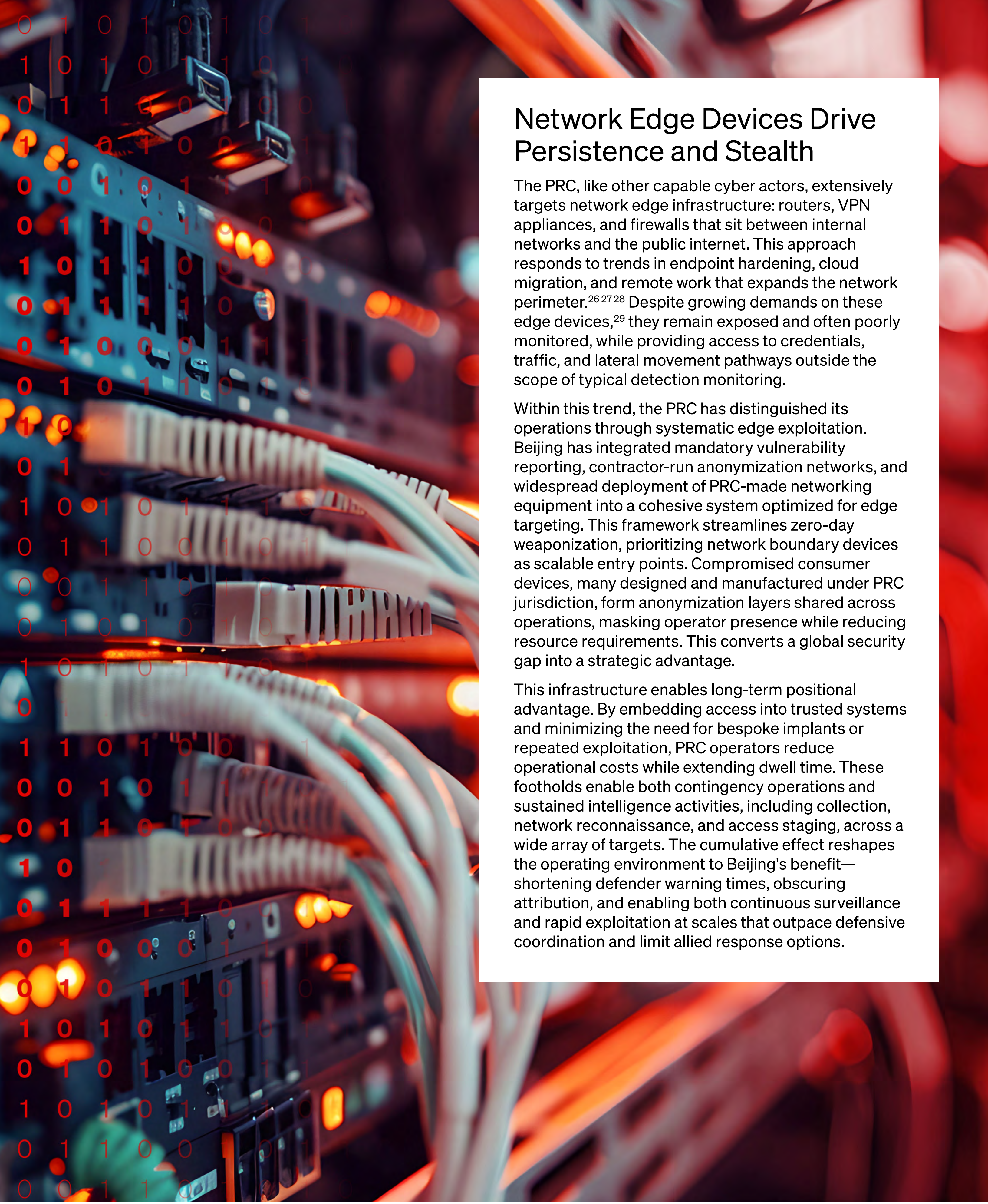
- **PRC operators are embedding software delivery compromises within regionally trusted platforms to gain access to political, economic, and strategic technology targets.** Rather than targeting globally distributed consumer applications, these operations compromise software distribution pathways tied to domestic, jurisdictionally proximate, or sector-specific platforms. This approach enables malware delivery via allowlisted update channels, conceals malicious activity within expected network behavior, and abuses trust in local vendors.

- Between 2020 and 2021, **Evasive Panda** targeted users in mainland China by abusing the update mechanisms of domestically developed applications, including Tencent QQ. The group delivered its malware through legitimate software infrastructure, likely by compromising internal distribution systems or intercepting traffic at the network level. Victims included members of an international NGO active in several provinces.[21]

- In 2023, **Evasive Panda** compromised DNS infrastructure at a Hong Kong internet service provider to redirect software update requests from media tools like 5KPlayer and YoutubeDL, which are used for video playback and content acquisition.[22]

- In 2023–2024, **PlushDaemon** compromised the software distribution process of IPany, a South Korean VPN provider, to deliver malware to a South Korean semiconductor company, a software development firm, and users in South Korea, Japan, and the PRC.[23]

- Between 2022 and 2024, **TheWizards** hijacked update mechanisms for PRC-made software such as Tencent QQ by manipulating IPv6 network configuration protocols to redirect traffic.[24] The group used adversary-in-the-middle techniques to deliver malware from spoofed update servers, targeting users in the mainland PRC, Hong Kong, and Southeast Asia.[25]

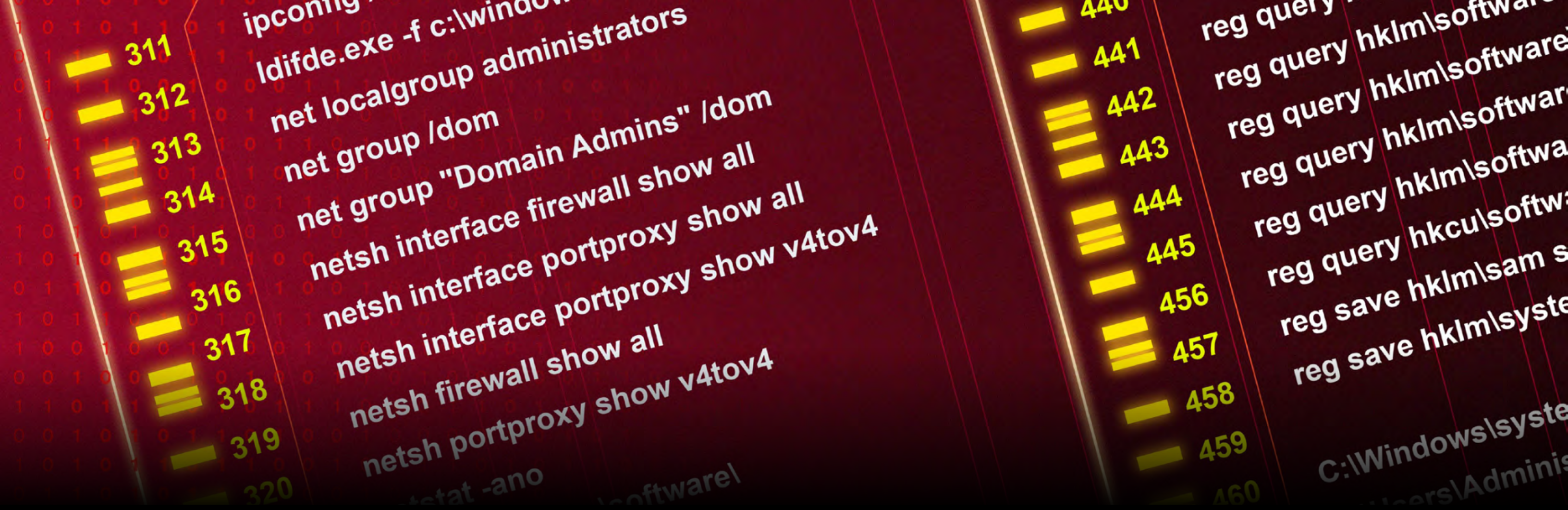


Network Edge Devices Drive Persistence and Stealth

The PRC, like other capable cyber actors, extensively targets network edge infrastructure: routers, VPN appliances, and firewalls that sit between internal networks and the public internet. This approach responds to trends in endpoint hardening, cloud migration, and remote work that expands the network perimeter.[26][27][28] Despite growing demands on these edge devices,[29] they remain exposed and often poorly monitored, while providing access to credentials, traffic, and lateral movement pathways outside the scope of typical detection monitoring.

Within this trend, the PRC has distinguished its operations through systematic edge exploitation. Beijing has integrated mandatory vulnerability reporting, contractor-run anonymization networks, and widespread deployment of PRC-made networking equipment into a cohesive system optimized for edge targeting. This framework streamlines zero-day weaponization, prioritizing network boundary devices as scalable entry points. Compromised consumer devices, many designed and manufactured under PRC jurisdiction, form anonymization layers shared across operations, masking operator presence while reducing resource requirements. This converts a global security gap into a strategic advantage.

This infrastructure enables long-term positional advantage. By embedding access into trusted systems and minimizing the need for bespoke implants or repeated exploitation, PRC operators reduce operational costs while extending dwell time. These footholds enable both contingency operations and sustained intelligence activities, including collection, network reconnaissance, and access staging, across a wide array of targets. The cumulative effect reshapes the operating environment to Beijing's benefit—shortening defender warning times, obscuring attribution, and enabling both continuous surveillance and rapid exploitation at scales that outpace defensive coordination and limit allied response options.



```
ipconfig
ldifde.exe -f c:\windo
net localgroup administrators
net group /dom
net group "Domain Admins" /dom
netsh interface firewall show all
netsh interface portproxy show all
netsh interface portproxy show v4tov4
netsh firewall show all
netsh portproxy show v4tov4
netstat -ano
software\
```

```
reg query
reg query hklm\software
reg query hklm\software
reg query hklm\softwar
reg query hklm\softwa
reg query hkcu\softw
reg save hklm\sam s
reg save hklm\syste
C:\Windows\syste
ers\Adminis
```

Leadership in Zero-Day Exploitation

Beijing has emerged as the global leader in zero-day exploitation targeting network edge devices. Since 2021, PRC-linked threat actors have dramatically increased their use of zero-day exploits, with 85% of the known vulnerabilities they targeted involving network edge infrastructure such as firewalls, VPNs, and routers.[30] This focus reflects a strategic interest in scalable access vectors that offer both persistence and prepositioning. In 2023 and 2024, PRC cyber operators were the most frequent users of zero-days across all software categories.[31 32] The UK's National Cyber Security Centre (NCSC) has since described zero-day exploitation as the "new normal," a shift that has helped the PRC increase its operations' volume and targeting precision.[33]

- In 2022, at least three PRC groups exploited a zero-day vulnerability in Sophos firewalls to gain access to select targets, including Tibetan organizations and a government department involved in Belt and Road Initiative (BRI)[b] debt negotiations.[34] The campaign demonstrated narrow targeting and alignment with PRC geopolitical priorities.
- Between late 2022 and 2023, a PRC threat group exploited a previously unknown vulnerability in Fortinet FortiGate devices to compromise over 20,000 systems globally. Victims included governments, international organizations, and defense contractors, highlighting the scalability and systemic risk posed by edge device exploitation.[35 36]
- In 2024, Google Threat Intelligence attributed five zero-day exploits to PRC-backed groups, all of which targeted security and network appliances.[37] This reinforces Beijing's sustained emphasis on edge infrastructure as a scalable and privileged access vector. Google found that PRC operators remain the most consistent state-linked exploiters of zero-days.

The PRC's regulatory model for vulnerability discovery provides cyber operators with a systematic and accelerated path to zero-day exploitation. A 2021 policy shift requiring rapid internal disclosure of software vulnerabilities has created a pipeline from private researchers to government-linked offensive units. This structure, which encompasses ministries, MSS contractors, PLA-affiliated labs, and academic institutions, consolidates insight and ensures that vulnerabilities can be rapidly evaluated, weaponized, and deployed. By integrating discovery with operational use, Beijing has positioned itself to exploit critical flaws before they are independently identified or patched, challenging conventional defensive timelines.

- PRC regulations require companies to report newly discovered software vulnerabilities to the Ministry of Industry and Information Technology (MIIT) within 48 hours. These disclosures are distributed across state-linked entities involved in offensive cyber activity, including the MSS and PLA.[38]
- Some PRC researchers have submitted vulnerabilities to international bug bounty programs after the state has already operationalized them, potentially as a sanctioned tactic to shape perception or, in some cases, as an unsanctioned attempt at financial gain.[39]

[b] **The Belt and Road Initiative** (BRI) is a global infrastructure and economic development initiative launched by the PRC in 2013 to enhance regional connectivity and expand trade across Asia, Africa, and Europe. It has significantly increased Beijing's geopolitical influence, though critics argue it can create debt dependency in participating countries, raising concerns about sovereignty and long-term economic sustainability.

Creation of Scaled Anonymization Networks

PRC cyber operators are using anonymization networks to obscure attribution, evade defenses, and blend into target environments. These Operational Relay Box (ORB) networks—composed of compromised routers, IoT devices, and leased infrastructure—allow malicious traffic to appear routine and locally sourced. PRC actors increasingly route operational traffic through devices located near or within the target's ISP, undermining geofencing heuristics and making detection harder.[40] Static, IP-based defenses struggle to track these constantly shifting mesh networks, which regenerate compromised nodes across tens or hundreds of thousands of devices.[41] This approach reflects both operational opportunism and the strategic utility of obfuscation in long-running access campaigns.

- In 2021–2022, **TAG-38** used compromised digital video recorders and security cameras in Taiwan and South Korea to route traffic while breaching Indian power infrastructure. These hop points provided proximity to the target and masked external traffic as trusted local connections.[42]
- In 2024, CISA observed that **APT40** was using compromised small home and office (SOHO) routers to proxy its operations targeting Australian entities. Many of the devices were either unpatched for known vulnerabilities or not patchable due to being past end-of-life.[43]
- In a multiyear campaign disclosed in 2025, **Weaver Ant** breached a major Asian telecommunications company while proxying its traffic through compromised routers operated by other regional telecom providers.[44] The adversary sustained persistent access to primary telecom target for four years.

The PRC's ORB networks reflect a broader ecosystem of provisioned infrastructure that supports scalable, persistent operations. PRC-linked contractors build and maintain these anonymization resources, replacing nodes as they are taken offline or blocked. This model reduces the operational burden on frontline actors and enables multiple campaigns to run in parallel with shared infrastructure. It also aligns with a longer-standing pattern in the PRC cyber ecosystem: outsourcing tools, platforms, and infrastructure while maintaining strategic flexibility and deniability.

- Between 2022 and 2023, Integrity Technology Group, an established PRC cybersecurity contractor, allegedly provided **Flax Typhoon** with access to a 260,000-node botnet of compromised consumer devices. This botnet included a user interface allowing clients to select nodes and issue commands remotely.[45][46]
- While the extent of state tasking is unclear, this model allows the PRC to scale access operations while distancing state actors from direct technical implementation. Similar infrastructure-as-a-service dynamics have underpinned many PRC campaigns since the early 2010s.[47][48]

PRC-made Networking Devices in Critical Sectors

The use of PRC-made networking hardware in U.S. government, defense, and critical infrastructure environments presents a long-term operational risk, even in the absence of confirmed compromise. This risk stems from both demonstrated adversary capability and structural opacity. PRC state-backed operators have repeatedly exploited vulnerabilities in networking devices, including backdoors and zero-days. While no public evidence confirms that backdoors in commercially sold PRC-made routers are deliberately implanted, their existence—intentional or not[49]—creates persistent access opportunities and affords plausible deniability to manufacturers. The concern is especially acute in sectors with limited device-level visibility or procurement processes that fail to account for supplier risk, where such equipment may quietly persist beyond the reach of standard audits or patch management. Recent discoveries in U.S. critical infrastructure (e.g., energy sector and ports) suggest this is part of a broader strategy: PRC-manufactured devices may include undocumented capabilities that compound long-term exposure in critical systems.

- PRC-headquartered network equipment manufacturing company TP-Link's share of the U.S. small-office/home-office (SOHO) router market grew from 20% in 2019 to 65%[c] in 2024.[50] Procurement records show that TP-Link routers are in use in U.S. government organizations including the Defense Logistics Agency, Naval Undersea Warfare Center, and NASA.[51]
- A 2022 Georgetown study found that, between 2015 and 2021, 1,681 state and local entities, including governments, utilities, universities, hospitals, and transit organizations, had procured foreign-made information and communications technology and services (ICTS) prohibited on federal networks, noting that Huawei routers and networking equipment were often purchased.[52]
- A 2022 investigation identified multiple undocumented backdoors in Jetstream and Wavlink routers, both manufactured by PRC-based Winstars Technology and sold in U.S. retail channels.[53] The routers reportedly contained hidden remote access interfaces and exposed administrative credentials that could be retrieved by unauthenticated users.
- A 2025 study reportedly discovered undocumented communication devices, including cellular radios, embedded in PRC-manufactured solar power inverters and batteries, creating potential channels to bypass firewall protections (e.g., blocking direct device communication with PRC IP addresses) and remotely alter device behavior.[54] Separately, U.S. national security officials have raised concerns that PRC-made ZPMC[d] ship-to-shore cranes—used at ports across the country, including those supporting military logistics—contain sensors not fully disclosed in procurement documentation.[55] A House investigation further found that ZPMC[d] had "repeatedly" requested remote access to its cranes with a "particular focus" on West Coast installations.[56] These capabilities could plausibly enable the tracking of cargo movements or disruption of port operations. Neither case has been publicly linked to PRC state-directed cyber offensive activity.

[c] TP-Link disputes the 65% market-share figure reported by the Wall Street Journal in December 2024. The firm refers to separate market research report finding 36.5% consumer unit market-share. Research did not locate the original report. (Source: https: //www. tp-link. com/us/landing/fact-sheet/)

[d] **Shanghai Zhenhua Heavy Industries Co**., typically referred to as **ZPMC**, is a PRC state-owned manufacturer that produces approximately 80% of the ship-to-shore (STS) cranes used at U.S. ports and 75% of STS cranes globally. It is a subsidiary of China Communications Construction Company, a key contractor in the Belt and Road Initiative. (Source: https: //www .wsj. com/ politics/national-security espionage-probe-finds-communications-device-on-chinese-cargo-cranes-867d32c0)

The PRC has a history of leveraging stolen source code and zero-day exploits to compromise widely deployed networking equipment. Past campaigns by PRC state-linked actors illustrate how access to firmware, encryption modules, or maintenance pathways can be abused for persistent compromise. These precedents suggest that even when a device is not explicitly backdoored at the point of manufacture, PRC operators may still exploit its supply chain, software, or support infrastructure for later-stage access.

- In 2012, **APT5** stole firewall source code from U.S.-based Juniper Networks and altered VPN encryption parameters, potentially enabling long-term traffic decryption. In 2014, the group added a remote-access backdoor to affected devices.[57]
- In 2021, **APT5** exploited a zero-day in Pulse Secure VPN appliances to compromise defense contractors, government entities, and financial institutions in the U.S. and Europe.[58]

The persistent infiltration of counterfeit PRC-made networking devices into critical U.S. systems presents additional security risks. Counterfeit or gray-market PRC devices often contain unauthorized hardware and pirated firmware, making them difficult to patch and vulnerable to tampering. These devices are typically not visible in official vendor support ecosystems, complicating vulnerability management and increasing the likelihood of unmonitored compromise. Their distribution within U.S. critical infrastructure, including operational Department of Defense (DOD) systems, magnifies the potential impact of compromise or malfunction.

- Since at least the early 2000s, counterfeit PRC-made network hardware has infiltrated U.S. military, government, and critical infrastructure supply chains, including systems used by the Navy, Treasury, and major defense contractors. A 2008 FBI investigation known as Operation Cisco Raider recovered over 3,500 fake routers, raising concerns about potential backdoor access and systemic supply chain exposure.[59][60][61]
- From 2014 to 2022, a U.S.-Turkish dual national and co-conspirators imported counterfeit Cisco devices from the mainland PRC and Hong Kong. These systems contained unauthorized parts and pirated software.[62] The counterfeit equipment was deployed in U.S. hospitals, schools, and classified DOD systems, introducing risks related to unauthorized access, degraded system performance, and lack of access to vendor patches or validated firmware updates.

AI Accelerates Operational Tempo

AI is turbocharging the scale, tempo, and targeting of PRC cyber and information operations. Beijing is integrating AI to overcome long-standing constraints in linguistic reach, analytic throughput, and operational scalability. These tools assist PRC operators in triaging vast multilingual datasets, automating aspects of technical reconnaissance, and accelerating the production of tailored influence content. Even in its early stages, AI is changing how the PRC collects intelligence, targets operations, and shapes global narratives, aligning with Beijing's "intelligentized" warfare doctrine that prioritizes data-driven decision-making and information dominance.[63]

This evolution erodes U.S. strategic advantage. By reducing friction in surveillance, exploitation, and influence activities, AI enables persistent activity with fewer indicators and shorter warning cycles. PRC actors can now act earlier, move faster, and hide more effectively. This accelerates campaign tempo, shrinks defenders' decision windows, and complicates attribution. These cumulative advantages make it increasingly difficult for the US and allies to coordinate responses, act decisively, and manage escalation effectively.

Overcoming Roadblocks to Intelligence Research and Analysis

The PRC's intelligence services are applying AI to overcome longstanding constraints in multilingual analysis, data triage, and real-time monitoring. These capabilities allow operators to more efficiently process open-source and stolen datasets, correlate multi-source surveillance streams, and extract insights from large unstructured data lakes. PRC analysts have publicly acknowledged that AI may help overcome deficits in foreign language and cultural expertise, long seen as a constraint on intelligence and influence operations.[64] AI integration appears aimed at improving elite surveillance, geopolitical risk sensing, and intelligence-driven targeting across both human and technical domains.

- **Multi-source surveillance correlation:** The PRC's reported use of AI to rapidly correlate surveillance data streams likely marks a pivotal shift in its ability to integrate and act on intelligence at scale. The MSS reportedly uses AI tools to generate near-instantaneous digital dossiers that fuse surveillance footage, cellphone metadata, license plate recognition, transaction logs, and travel records.[65] These outputs likely support individual monitoring, operational targeting, and rapid risk profiling for internal security and foreign counterintelligence missions. By accelerating the fusion of multi-source surveillance, AI enables faster, more tailored responses to perceived threats, reducing latency in decision-making and tightening the loop between data collection and action.
- **Social media monitoring and sentiment analysis:** According to a 2025 OpenAI report, a PRC-based network dubbed "**Peer Review**" used large language models[e] (LLM) to translate protest-related content, analyze English-language screenshots, and debug code for a proposed AI-powered social media monitoring tool. In promotional materials refined using ChatGPT, the operators described the system, called the "Qianyue Overseas Public Opinion AI Assistant," as capable of ingesting content from platforms such as X, Telegram, and Reddit to identify overseas discussions about PRC political topics. These materials also claimed that the resulting insights had been passed along to PRC embassies and intelligence agents monitoring protests abroad.[66]
- **Exploitation of large-scale breach data:** In the 2010s, PRC data theft operations systematically collected large, consistently structured data like security clearance paperwork, travel records, and credit reports. More recently, by contrast, PRC threat actors, accelerated by the nationalized zero-day vulnerability pipeline, have increasingly conducted smash-and-grab intrusions that yield massive, unstructured, and multilingual datasets.[67] This transition is likely driven by AI tools, which enhance their ability to extract actionable intelligence from such disparate unstructured data pools — especially inboxes, document archives, and communications seized from foreign defense, diplomatic, and political institutions.
- **Automation of technical reconnaissance:** Groups like **SweetSpecter** and **Charcoal Typhoon** have reportedly used LLMs to automate portions of vulnerability analysis, malware debugging, and phishing content generation.[68] This reduces manual workload and likely accelerates cycles of reconnaissance, exploit development, and operational adaptation.
- **Translation and technical content exploitation:** AI-enabled translation platforms are used to accelerate exploitation of non-Chinese-language technical materials, including cybersecurity reports, academic papers, and technical documentation. Operators such as **Salmon Typhoon** have leveraged these capabilities to assess foreign tools, vulnerabilities, and methods relevant to PRC cyber operations and defense planning.[69]

[e] **A large language model** (LLM) is a type of artificial intelligence trained on extensive datasets that include both natural and programming languages; in cybersecurity, LLMs can support tasks such as phishing content generation, malware debugging, and vulnerability analysis by interpreting or generating human-readable and machine-readable text."

Scaling, Accelerating, and Tailoring Influence Operations

The People's Liberation Army (PLA) sees AI as central to its vision of cognitive warfare and information dominance.[70] PLA doctrine describes AI as essential to shaping adversary decision-making, degrading social cohesion, and asserting "discourse power" abroad.[71] AI-enabled information operations are framed as tools to influence both wartime and peacetime strategic competition, used to manipulate public perception, destabilize adversaries, and expand Beijing's narrative control over contested geopolitical issues.[72]

PRC actors are using AI-generated content to overcome structural barriers that have long constrained Beijing's reach in foreign information environments. Content generation models drastically reduce the labor cost of producing large volumes of narrative-aligned material while enabling automated variation that helps evade platform detection systems. PLA-affiliated writings emphasize that AI tools help compensate for organizational weaknesses in scaling foreign-language production and using cultural nuance, professed longstanding deficiencies in PRC influence efforts.[73][74] AI enables influence operations to deploy at a speed, volume, and contextual precision that would previously have required significant time or human capital investment, narrowing the defensive margin that once came from Beijing's reliance on limited skilled personnel.

- In late 2024, a PRC-originating actor, likely **Spamouflage**, used ChatGPT to generate anti-U.S. articles in Spanish, which were then published in mainstream Latin American media outlets. OpenAI identified this campaign as the first confirmed use of its tools to plant AI-generated content in traditional media.[75]

AI is enabling PRC influence networks to scale operations, target audiences more precisely, and reduce their reliance on manual oversight. Large language models are being used to analyze foreign social media environments, profile audiences, and tailor content to local contexts, amplifying polarization and deepening mistrust. PLA researchers envision real-time, adaptive campaigns powered by autonomous bots and generative models.[76][77] Field activity suggests this vision is already being tested, with early deployments showing signs of automated engagement and comment generation, though prompt artifacts reveal lingering operational limitations.

- A 2025 Google report found that PRC-linked actors, including **Dragonbridge**, were using generative AI to refine the framing, tone, and timing of social media posts, particularly in Australia and the United States.[78] The use of models like Gemini reportedly enabled fine-tuned messaging toward diaspora populations and other local audiences.
- In 2024, social media accounts tied to the **Green Cicada** network, which has suspected PLA connections, repeatedly posted content that included prompt artifacts such as "As an AI language model…" or "Here is a possible comment in English mimicking the provided Tweet."[79] These errors suggest testing of AI-generated comment automation that lacked proper prompt filtering or post-processing safeguards.
- PRC investments in domestic-facing AI systems, like the "AI Rumor Crusher," also highlight the regime's technical ambition in real-time narrative adjudication and dissemination tracing.[80] Developed by the Cyberspace Administration of China (CAC) and praised in PLA writings, the system uses natural language processing (NLP) and reinforcement learning[f] to identify rumors, assess source credibility, and infer motivation, demonstrating capabilities that could be extended or adapted for external-facing operations.

Synthetic media, including AI-generated video and audio, is also being incorporated to enhance the emotional impact, deniability, and realism of PRC online influence efforts. These techniques enable the creation of fabricated personas, forged endorsements, and falsified reporting that can mislead audiences and erode trust in authentic voices.

- Since at least 2023, the **Spamouflage** network has used AI-generated avatars posing as news anchors in English-language videos that deliver pro-Beijing messages.[81]
- In January 2024, **Dragonbridge** used AI-generated audio to fabricate a political endorsement from former Taiwanese presidential candidate Terry Guo, timed to coincide with Taiwan's national election day, likely to sow confusion or shift last-minute voter sentiment.[82]

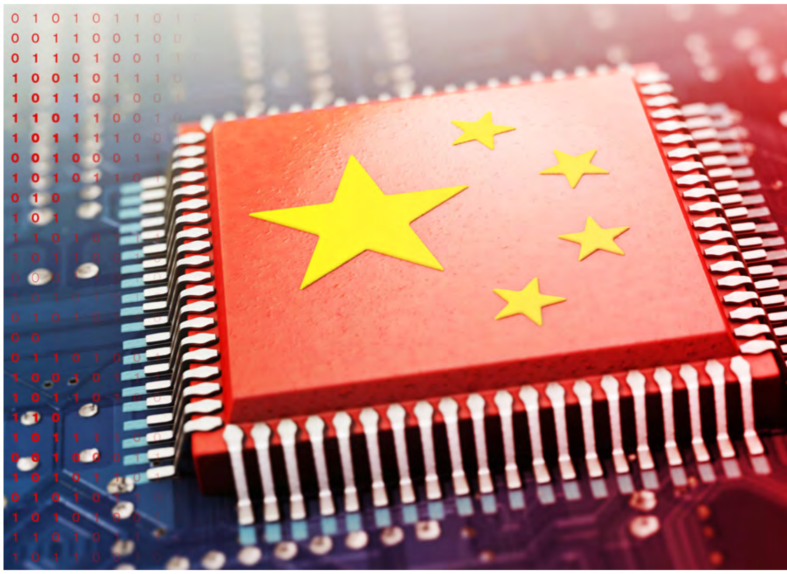
Overcoming AI Bottlenecks

Beijing is using cyber operations to mitigate structural bottlenecks in its pursuit of global AI leadership. Despite whole-of-state efforts—including industrial policy, talent recruitment, and illicit procurement—the PRC faces persistent obstacles to acquiring the intellectual property, talent, and hardware required for AI dominance.[83] Cyber-enabled theft offers a strategic workaround where legal and commercial pathways fall short, targeting current-generation systems as well as the research foundations and personnel pipelines needed to sustain long-term technological independence. These operations may help close short-term gaps, but they cannot fully offset deeper structural limitations.

- The PRC faces persistent challenges in acquiring the intellectual property and human capital necessary for cutting-edge AI development. A 2018 multi-country study found that PRC computer science graduates, even from top institutions, underperformed their U.S. counterparts on standardized AI competency assessments, highlighting a persistent talent gap despite large investment in STEM education.[84]
- PRC-affiliated cyber actors have targeted foreign AI research institutions and tech companies for intellectual property theft. Groups such as **UNK_SweetSpecter** have focused on extracting proprietary algorithms, model architectures, and training datasets, likely aiming to reverse-engineer or replicate high-performance AI systems developed abroad.[85] [86]

The PRC's reliance on foreign semiconductor supply chains has made advanced chip fabrication a top-tier cyber espionage priority. High-performance semiconductors are critical to training and running modern AI systems. U.S.-led export controls have denied the PRC access to the most advanced chips and chipmaking tools, especially extreme ultraviolet (EUV) lithography.[87] In response, PRC cyber operators have attempted to compromise firms positioned at key nodes in the global semiconductor ecosystem. While cyber operations have primarily focused on front-end design and fabrication firms, assembly, test, and packaging (ATP) processes represent a structurally vulnerable point in the supply chain, with heavy concentration in the PRC and Taiwan and close integration with the upstream design and fabrication processes.[88]

- U.S. and allied export restrictions have sharply constrained the PRC's access to advanced chips. These restrictions include prohibitions on the sale of EUV lithography equipment from Dutch firm ASML and high-end GPUs from U.S. firms, components essential for fabricating or operating large-scale AI models.
- Beijing has responded with cyber intrusions linked to groups like **Chimera**, **APT41**, and **APT17** targeting semiconductor firms in countries like Taiwan, South Korea, and the Netherlands.[89] These efforts complement PRC-linked insider threat and talent poaching efforts.[90]
- Despite these efforts, the PRC remains highly dependent on imported high-performance chips. After a pandemic-era dip driven by inventory corrections, the PRC's semiconductor imports rebounded to pre-2020 levels by 2024, underscoring the continued gap between domestic capacity and demand.[91] [92]



Contesting Attribution Preserves Escalation Control

Beijing sees attribution as strategic terrain. Public attribution establishes responsibility, signals awareness to both the responsible government and external audiences, and frames the political conditions for potential diplomatic, legal, or military responses. PRC strategists view this as foreign coercion—a tool to impose norms, undermine legitimacy, and restrict PRC policy options.[93]

This perspective shapes both the PRC's operational tradecraft and its information strategy. Beijing leverages criminal proxies, generic toolsets, and obfuscated infrastructure to frustrate forensic attribution, while orchestrating state and private-sector disclosures to simulate attribution consensus and reinforce counter-narratives. These performative efforts mimic the U.S. name-and-shame model[g] but substitute curated, limited, and sometimes likely fabricated material for verifiable evidence. The aim is likely to shape perceptions and secure a political advantage by undermining the credibility of foreign attribution and fracturing collective response.

Control over attribution narratives enhances Beijing's ability to shape escalation dynamics.[h] In a private December 2024 diplomatic exchange, a senior PRC official reportedly suggested that **Volt Typhoon** intrusions in U.S. critical infrastructure were linked to rising American support for Taiwan—an unusual departure from Beijing's usual denials.[94] Rather than fully acknowledging responsibility, the PRC used carefully ambiguous language to imply escalation risk while preserving deniability. This selective posture shift demonstrated how attribution narratives can serve as tools of coercive signaling. By maintaining ambiguity, Beijing preserves flexibility to escalate, test boundaries, or disengage while reducing the risk of decisive retaliation—using attribution control to shape both perception and escalation dynamics..

This dynamic reduces U.S. ability to respond with speed, clarity, and alignment. Contested attribution causes allied hesitation, blurs legal thresholds, and fragments collective action. Deterrence also weakens: if Beijing's role is too ambiguous, its threats lose weight; if it is too clear, it risks triggering costs it prefers to avoid. Strategic ambiguity lets Beijing navigate this space on its terms. By shaping attribution, Beijing shapes perception, pace, and consequence. It chooses when pressure is applied, when escalation is threatened, and when to retreat. By shaping attribution narratives, Beijing shapes initiative in competition and constrains U.S. freedom to act.

Blurred Lines Between Criminal and State Groups

The PRC relies on a dense ecosystem of domestic contractors and tolerated cybercriminals that fuse state direction with illicit activity. These actors perform espionage, disruption, and monetization side by side, often supporting government tasking while pursuing private gain. By embedding intelligence activity within criminal tradecraft and infrastructure, PRC entities complicate attribution, expand operational flexibility, and preserve deniability.[95] This approach echoes Beijing's pattern of opportunistically leveraging organized crime outside the mainland[i] to advance state goals, such as attacking pro-democracy protesters in Hong Kong and harassing independence supporters in Taiwan.[96] [97] [98]

[g] **"Name and shame"** refers to a tactic in which a government publicly attributes cyber operations to state sponsors and sometimes to specific individuals like government personnel or contractors. While often framed as an enforcement measure aimed at imposing reputational costs to deter malicious cyber activity, its effectiveness in compelling behavioral change is widely debated. Instead, these attributions often serve broader strategic functions, including signaling deterrence, justifying legal actions, rallying allied support for sanctions, and shaping international norms around acceptable state behavior in cyberspace.

[h] The PLA's doctrinal concept of escalation management is **"effective control"** (有效控制, yǒuxiào kòngzhì), which emphasizes managing the intensity, timing, and scope of military operations to achieve political objectives while avoiding unintended escalation. For a deeper discussion of significance of the PLA's escalation and crisis management doctrine refer to https://asiasociety.org/policy-institute chinas-views-escalation-and-crisis-management-and-implications-united-states.

[i] **"Mainland China"** refers to PRC-claimed territories that are neither special administrative regions (Hong Kong, Macau) or nor Taiwan. Crucially, these areas are outside the full administrative control of the PRC government.

- Since at least the early 2010s, **APT41**[j] has operated as both a state-linked espionage contractor and a financially motivated criminal group, often performing state-aligned operations during work hours while engaging in profit-driven campaigns in parallel.[99] APT41 has fused espionage and criminal gain within the same campaigns, such as stealing code-signing certificates from video game firms for operational use while also exploiting those firms' in-game currencies for profit.[100]

- A 2024 leak of internal files from contractor **i-Soon** exposed how it supported PRC government clients through on-demand offensive operations, data sales, and surveillance operations.[101] Low pay, lax oversight, and fierce competition pushed the firm into illicit activity, including bribery, collusion, and coordination with criminal networks. The government appeared to tolerate these practices so long as political loyalty was maintained and tasking was fulfilled.

Beijing's tolerance and likely quiet cultivation of foreign criminal networks strengthens its ability to project influence through unofficial channels while shielding state organs from exposure. In both cyberspace and the physical world, PRC-linked actors appear to benefit from the infrastructure, tradecraft, ingenuity, and deniability that criminal intermediaries provide. Ethnic-Chinese mafias in Europe and Southeast Asia have facilitated surveillance, repression, and political interference aligned with Beijing's interests, while also sustaining illicit finance and logistics pipelines that state-linked cyber operators can quietly repurpose.[102] [103] [104] Beyond tactical support, they enable scalable access to global infrastructure, coercive leverage over diaspora communities, and informal pathways to disrupt adversaries' supply chains and information environments. The result is a model in which transnational organized crime serves as a durable gray zone ecosystem advancing Beijing's strategic objectives with limited attribution risk.

- Around 2023, PRC actors reportedly acquired inauthentic social media personas from Southeast Asia-based criminal networks to rebuild covert influence infrastructure.[105] These accounts were used to amplify divisive narratives in Australia, targeting domestic critics of the PRC and spreading falsified content on politically sensitive topics. Messaging included attacks on researchers, companies, and institutions viewed as hostile to Beijing's interests.[106]

- Since June 2022, Russia-based cyber extortion group **BianLian**[k] has targeted Australian critical infrastructure, professional services, and property sectors, alongside U.S. critical infrastructure in multiple sectors.[107] In March 2024, it breached Northern Minerals, an Australian rare earths firm[l] developing PRC-alternative supply chains, and leaked sensitive data days before Canberra ordered PRC-linked divestment.[108] [109] The timing raises questions about whether Beijing may be indirectly leveraging Russia-based criminal groups to track or disrupt decoupling efforts, in addition to its own domestic criminals.

PRC state-aligned operators have employed tactics resembling financially motivated cybercrime in operations involving espionage, disruption, and possible coercive signaling. Criminal tradecraft offers operational advantages: it enables scale without bespoke infrastructure, lowers the technical barrier to deployment, and cloaks state operations in ambiguity that can frustrate attribution. These qualities make it well-suited to shaping adversary behavior in politically sensitive contexts while reducing the risk of direct attribution or escalation.

- In 2020, **APT41** deployed wiper malware disguised as ransomware against Taiwanese semiconductor and chemical firms in the immediate lead-up to President Tsai Ing-wen second inauguration.[110] The campaign likely served a coercive signaling function while leveraging criminal tradecraft to deflect attribution.

[j] For more information about **APT41**, see the discussion of "Chengdu-based individuals" in Booz Allen's report *Same Cloak, More Dagger*, p. 41-43.

[k] **BianLian** is a cybercriminal group that, according to CISA, is "likely based in Russia, with Russia-based affiliates." Its name refers to a Chinese opera technique called "face-changing." (Source: https://cisa.gov/news-events/alerts/2024/11/20/cisa-and-partners-release-update-bianlian-ransomware-cybersecurity-advisory)

[l] For more information about PRC cyber operations targeting the global rare earths industry, consult Booz Allen report's *How to Succeed at Annexation Without Really Fighting*, p. 25-26. It details PRC efforts in Canada, Australia, Japan, and Brazil for more than a decade to retain Beijing's potent geopolitical lever, stemming from its dominance in rare earths extraction and processing.

- In November 2022, a ransomware attack crippled digital systems at India's All India Institute of Medical Sciences, disrupting care and exposing sensitive data.[111] Security firms attributed the incident to the **ChamelGang**, a PRC espionage group[m] that often deploys ransomware.[112 113] Indian officials confirmed the intrusion originated from PRC-based infrastructure, without assessing attribution.[114] The attack occurred during a period of elevated India-PRC tensions following clashes along their disputed border. Other Beijing groups targeted and possibly disrupted Indian critical infrastructure during this tense period.[n]
- Also in late 2022, a ransomware attack linked to **ChamelGang** targeted the office of the Brazilian president, disrupting operations and encrypting sensitive data.[115] The operation occurred as diplomatic tensions between Brazil and the PRC were elevated, with Beijing's officials publicly criticizing President Jair Bolsonaro's rhetoric and withholding key economic engagements.[116] The timing suggests the attack may have served as a form of coercive pressure during a period of fraying bilateral ties.
- In 2024, **APT41** launched a global phishing campaign that used traditional cybercriminal delivery tactics to pursue likely state-directed espionage objectives. The operation relied on mass-distributed lures impersonating tax authorities and leveraged public infrastructure, reflecting tradecraft more often seen in financially motivated campaigns. The targeting concentrated on sectors of long-standing intelligence interest to Beijing, including aerospace, insurance, chemicals, and manufacturing, suggesting a strategic espionage intent.[117]

[m] **ChamelGang** is a globally active PRC-aligned threat group. TeamT5, a security firm whose threat landscape awareness is highest in its headquartered-country Taiwan, observed that half of ChamelGang's known operations target governments and almost one-tenth target think tanks, which are more typically espionage than for-profit adversary targets. TeamT5 assesses that ChamelGang uses ransomware to "cover its tracks," rather than financially enrich itself. (Source: https://www.youtube.com/watch?v=ybWzRDGgpvw)

[n] For more information about the PRC's **cyber-enabled pressure against Indian critical infrastructure** related to the border conflict, consult Booz Allen's report *Same Cloak, More Dagger*. It examines a series of PRC-linked intrusions at Indian power grid operators between 2020 and 2022 that plausibly caused a power outage in Mumbai, as well as other activity at ports, a logistics provider, and the country's national emergency response system.

Increasingly Specific Counterclaims to Neutralize Foreign Allegations

Beijing is seeking to degrade the credibility of cyber attribution as a basis for coordinated diplomatic response. Faced with growing multilateral alignment around technical evidence, the PRC has shifted from blanket denials to more targeted efforts to undermine the legitimacy of specific attribution claims. PRC officials now routinely frame foreign allegations as technically flawed and politically motivated, reinforcing a strategic narrative of victimhood and bias.[118] This approach allows Beijing to delay or defuse international responses without needing to disprove claims directly.

- In response to the 2021 joint U.S.-European Union (E.U.) attribution of the Microsoft Exchange breaches to PRC-linked actors, publicly tracked as **Silk Typhoon**,[119] Beijing claimed the accusations were "fabricated out of thin air" and lacked a "complete chain of evidence."[120]
- Following 2024 U.S. indictments of **APT31** operators, a PRC spokesperson dismissed the case as based on "inadequate" British evidence that lacked "professionalism."[121]
- In a 2024 joint advisory naming **APT40**, the Five Eyes, Germany, Japan, and South Korea reiterated links between the group and **The PRC's Ministry of State Security (MSS)**. Beijing denied the allegations and questioned the technical basis of the findings.[122]

The PRC is institutionalizing counter-narratives by embedding them in state-linked threat reporting and media cycles. Since 2022,[123] PRC authorities and affiliated cybersecurity firms have increasingly released technical reports alleging U.S. cyber intrusions.[124] [125] [126] [127] These publications are structured to mimic industry threat intelligence but often lack original findings or verifiable sourcing. By presenting these reports as neutral analysis and then amplifying them through state media and official spokespersons, Beijing seeks to add credibility to its narrative that the PRC is a cyber victim and cast foreign attribution efforts as hypocritical and politically motivated. These technical allegations complement Beijing's well-worn boilerplate dismissal of attribution accusations.

- Beijing has long dismissed foreign accusations as "groundless" and politically motivated, insisting that the PRC "firmly opposes and combats all kinds of cyberattacks."[128] [129] Officials frequently invoke the Chinese idiom of a "thief crying stop thief"[130] to suggest that others engage in the very behavior they accuse the PRC of.[131] [132]
- In 2022, the PRC Foreign Ministry recycled decade-old allegations of intrusions in the country by U.S. operators as novel evidence of misconduct.[133] [134]
- In October 2024, a PRC-affiliated cyber report recast previously attributed PRC state-linked offensive prepositioning group **Volt Typhoon** as an "international ransomware operation,"[135] contesting U.S. claims of state sponsorship[136] and exploiting narratives about PRC use of cybercriminal proxies.

Beijing is coordinating state and private-sector disclosures to simulate attribution consensus and reinforce counter-narratives. This tactic mimics U.S. name-and-shame model but substitutes curated or potentially manipulated material for verifiable intelligence. The aim is to fabricate an appearance of independent validation and bolster Beijing's credibility, particularly when pushing counterclaims involving Taiwan or the United States. Increasingly, these disclosures rely on *false equivalence*; they cast intelligence collection against traditionally legitimate targets as comparable to the PRC's own prepositioning to disrupt civilian infrastructure. The strategy exploits ambiguity to blur the lines between espionage and laying the groundwork for sabotage, hoping to erode support for coordinated diplomatic responses.

- In 2022, PRC media engaged in what appeared to be disclosure theater, portraying normatively acceptable and acknowledged U.S. intelligence activity as major revelations. In 2022, they named a senior U.S. cyber operator, as if revealing a covert actor[137] despite the intelligence community having long widely acknowledged this individual's former affiliation.[138] [139] In 2023, outlets reported on alleged U.S. government phishing of a PRC university[p] [140] but declined to include the context that the institution is a core national defense research hub, a typically uncontroversial collections target.[141]

[p] The alleged victim, **Northwestern Polytechnical University**, is one of the PRC's top public military research universities (a.k.a., the "Seven Sons of National Defense") and describes itself as "devoted to improving and serving the national defence science (sic) and technology industry." (Source: https://unitracker.aspi.org.au/universities/northwestern-polytechnical-university/)

- In 2022, the **Dragonbridge** influence campaign[q] appeared to troll U.S. cyber attribution by promoting absurd claims that APT41 was a U.S. government-linked threat actor—an apparent attempt to demonstrate how easily attribution narratives can be fabricated.[142] It amplified these claims by crudely and transparently plagiarizing, altering, and mischaracterizing Mandiant threat reports and news coverage. It also created Twitter accounts that impersonated the counter-PRC attribution persona Intrusion Truth,[r] and deployed additional accounts to directly challenge Intrusion Truth's posts. The campaign likely sought to delegitimize attribution efforts by undermining trust in the attribution process through brazen, performative fabrications.
- In March 2025, the MSS publicly named four Taiwanese cyber operators linked to Taiwan's Information, Communications, and Electronic Force Command (ICEFCOM), accusing them of targeting PRC critical infrastructure and posing as the hacktivist persona "Anonymous 64."[143] [144] The announcement coincided with near-simultaneous publications by four PRC cybersecurity firms detailing related Taiwan-linked activity.[145] [146] [147] Booz Allen analysts note that some of the photos released by the MSS as evidence bore signs of possible AI generation, raising questions about fabrication and the authenticity of supporting material.
- In April 2025, the PRC's Cyberspace Security Association alleged that U.S. intelligence agencies had compromised a major PRC commercial encryption provider. The report, citing CNCERT analysis, claimed attackers had stolen source code and customer data tied to PRC government entities. PRC state-run newspaper the *Global Times* framed the operation as an attack on "critical infrastructure," quoting state-linked experts warning of potential supply chain backdoors and encryption degradation.[148] The narrative amplified increasingly frequent PRC claims that U.S. cyber operations target national infrastructure, while implicitly brazenly equating espionage against a government-connected encryption firm with PRC prepositioning in hospitals, ports, and power grids.
- In April 2025, the Harbin Public Security Bureau publicly named three alleged U.S. government cyber operators, accusing them of conducting "cyberattacks" on the 2025 Asian Winter Games, as well as energy, telecommunications, water, and defense-related academic institutions in Heilongjiang Province.[149] Concurrently, the National Computer Emergency Virus Response Center[150] and a private security firm[151] released reports on this alleged operation and other related activity. Collectively, the PRC's claims—presented with minimal technical substantiation—appeared to narratively "throw the kitchen sink" at the U.S.: alleging attempted disruption of the Games, espionage against athletes and defense institutions, targeting of critical infrastructure, exploitation of Windows backdoors, and publicly naming individual U.S. government operators. The PRC Foreign Ministry concurrently issued a call for the U.S. to "adopt a responsible attitude to cybersecurity" and "cease its groundless smears and accusations."[152]

[q] Mandiant uses the term "**influence campaign**" to collectively refer multiple instances of related information operations constituting a concerted effort often over an extended period. In this case, Dragonbridge is a "campaign," whereas the entity or individuals conducting the campaign would be an "actor" in its nomenclature. (Source: https://cloud.google.com/blog/topics/threat-intelligence/understand-action-intelligence-information-operations)

[r] **Intrusion Truth** is a pseudonymous persona that exposes the human and organizational side of PRC-linked cyber espionage groups via detailed blog posts. Its disclosures are highly reputable, frequently validated by later U.S. Department of Justice indictments of the same individuals and organizations.

Arenas

Undermining U.S. Agility and Escalation Control in East Asia

The PRC's eastern strategic periphery is a front line defined by technological dependencies, maritime disputes, and entrenched U.S. security relationships. These factors limit Beijing's ability to shape the regional order on its terms. In Taiwan, the South China Sea, and Japan, these pressures are acute: resilient democratic systems, hardened infrastructure, and increasingly coordinated alignment with the United States. Rather than accepting these limits, Beijing is contesting them—sometimes covertly, sometimes overtly, and always persistently. Cyber and information operations are its principal tools, avoiding direct confrontation while enabling access to infrastructure, influence over political ecosystems, access to intellectual property, and erosion of adversary cohesion.

Across the region, Beijing is using cyber and information operations to reduce the capacity of U.S.-aligned countries to respond quickly or cohesively to strategic pressure. In Taiwan, this includes efforts to degrade public resistance to unification and to preposition technical access for infrastructure disruption. In the Philippines and Vietnam, campaigns focus on mapping enforcement posture and shaping elite behavior around maritime disputes. In Japan, operations target the country's high-value technology sector and networks relevant to alliance coordination and defense logistics. These activities form a deliberate strategy of environmental shaping, designed to exploit peacetime access, strain political alignment, and build leverage for use in future regional conflicts.

Taiwan

PRC-linked influence operations during Taiwan's 2024 presidential election sought to undermine democratic legitimacy, discredit pro-sovereignty candidates, and distort perceptions of public sentiment. Messaging disproportionately targeted the Democratic Progressive Party (DPP)[s] and its candidate Lai Ching-te, portraying them as destabilizing U.S. proxies while amplifying pro-unification themes. The efforts' multi-pronged approach—combining AI-generated content, identity-based fearmongering, falsified polling data, and state-directed propaganda—reveals a political warfare strategy that leverages varied, scalable, and deniable tools to weaken Beijing's political opponents.

- In 2023–2024, Taiwanese authorities and civil society groups documented a wave of AI-generated content aimed at influencing the presidential election, much of it aligned with PRC strategic objectives. Fabricated content included deepfake videos and synthetic audio impersonating both current DPP leaders and opposition candidates (e.g., a fake audio clip of TPP candidate Ko Wen-je attacking the DPP), and AI-generated videos accusing DPP figures of corruption.[153] The Australian Strategic Policy Institute (ASPI) attributed several of these operations to PRC-linked networks, including **Spamouflage**, which used AI avatars, fake documents, and coordinated posts across platforms like TikTok, Douyin, and Facebook to discredit pro-independence candidates.[154]
- In the lead-up to Taiwan's January 2024 election, PRC government contractor **i-Soon** launched an influence campaign aimed at inflaming domestic unrest and disrupting Taiwan–India relations.[156] [157] The operation stoked xenophobic fears that a real pending labor agreement by the DPP government[158] would bring 100,000 Indian migrant workers to Taiwan and create public safety risks for women.[159] I-Soon operators seeded the narrative on local forums and amplified it across major social media channels, exploiting xenophobic tropes and anti-immigrant sentiment.
- PRC-linked state media orchestrated a coordinated influence campaign targeting Taiwanese voters on platforms such as Facebook and YouTube.[160] Messaging disproportionately attacked Lai Ching-te (portraying him as a U.S. puppet and likely to start a war) while simultaneously amplifying pro-unification narratives and apolitical cultural content to build audience rapport. PRC outlets also promoted fabricated stories, including claims of a U.S.-directed bioweapons lab in Taiwan. The campaigns relied on paid ads and suspected click farms to inflate reach, exposing Taiwan's continued struggle to regulate foreign political messaging.
- In late 2023, Taiwanese prosecutors uncovered a PRC-backed effort to fabricate and disseminate fake presidential polling data ahead of the 2024 election.[161] Under direction from a "Chinese agent," local actors created falsified poll results and promoted them via messaging apps and online news platforms.
- Consistent with an earlier predictive assessment by Booz Allen's analysts,[162] Taiwan's intelligence community determined that younger people became the primary targets for PRC-linked influence operations in 2023, focusing on platforms and outlets predominantly used by this demographic.[163]

Beijing is systematically embedding cyber access across Taiwan's civilian infrastructure, enabling pre-crisis coercion and the ability to accelerate disruption in a contingency. Activity since 2023 reflects an apparent operational shift toward infrastructure prepositioning across sectors with both military and societal significance, including telecom, healthcare, and transit. PRC operators appear to be developing coercive leverage intended for sub-threshold signaling, cost imposition, and asymmetric escalation control. In the event of a hot conflict, the PRC would likely exploit some of this access for disruptive attacks, consistent with doctrine that emphasizes the erosion of adversary cohesion through early-stage information dominance.

[s] **The Democratic Progressive Party** (DPP) is a major political party in Taiwan that promotes a distinct Taiwanese identity and affirms Taiwan's *de facto* sovereignty, opposing political unification with the PRC while avoiding a formal declaration of independence. The DPP has won Taiwan's presidency in three consecutive elections (2016, 2020, and 2024), though it lost its legislative majority in the 2024 election after holding it for two terms.

- Taiwan’s National Security Bureau (NSB) reported in 2024 that government agencies faced an average of 2.4 million “cyberattacks”[t] per day, nearly double the 2023 rate. Officials attributed the vast majority to PRC-linked actors, whose top targets were sectors likely to be immediately important in an armed conflict: telecommunications, transportation, and defense supply chain entities.[164] The 650% surge in targeting of telecommunications dwarfed the upticks in all other sectors,[165] consistent with PRC doctrinal emphasis on achieving information dominance in conflict.[166]
- In early 2025, a threat actor using the novel ransomware **CrazyHunter** launched a multi-sector campaign targeting entities across Taiwan. Victims included hospitals, a university, and firms involved in electronics, semiconductor components, and interior materials.[167][168] The attacks included the exfiltration and strategic release of stolen data online, suggesting that it was a hack-and-leak effort aimed at eroding public trust in institutions, fueling social anxiety, and degrading critical infrastructure resilience.[169] Taiwan’s law enforcement charged a PRC national employed at a “well known”[170] PRC cybersecurity firm for his alleged involvement, making this the first case of Taipei using name-and-shame against the PRC.[171] A public statement by Taiwan’s National Security Bureau appears to suggest that the PRC government was ultimately responsible for the operation.[172]
- Since at least 2023 and likely continuing into 2025, PRC-linked threat cluster **UAT-5918** has sought to achieve persistent access to critical infrastructure entities in Taiwan, including in the healthcare, telecommunications, and information technology sectors. The group exploited public-facing systems to establish long-term footholds and conducted extensive internal reconnaissance across victim networks.

PRC cyber operators are intensifying efforts to compromise Taiwan’s advanced technology sector to erode its strategic autonomy and gain asymmetric advantage. Recent campaigns have focused on extracting defense-relevant research, monitoring innovation pipelines, and mapping industrial dependencies. Targeting of Taiwan’s semiconductor, aerospace, and research institutions aligns with Beijing’s long-term objectives: securing access to critical technologies, reducing reliance on foreign innovation, and weakening Taiwan’s role in regional supply chains and security networks. These operations underscore the enduring vulnerability of Taiwan’s high-value tech assets to persistent cyber intrusion, particularly given their strategic overlap with U.S. and allied defense-industrial priorities.

- In mid-2023, **APT41** likely compromised an unspecified Taiwanese government-affiliated research institute, exfiltrating documents related to proprietary and sensitive computing technologies.[173]
- Between late 2023 and early 2024, **RedJuliett** targeted at least 75 Taiwanese organizations, with particular emphasis on the technology sector.[174] Confirmed and likely targets included a semiconductor firm, two aerospace companies under military contract, eight electronics manufacturers, a technology-focused research institute, two technology universities, an industrial embedded systems company, and seven computing industry associations. These efforts aligned with Beijing’s strategic interest in Taiwan’s critical technology ecosystem, including supply chains tied to defense, electronics, and advanced manufacturing.
- In mid-2024, **Tidrone** targeted Taiwan’s military technology supply chains, focusing on drone manufacturers and the satellite industry, in a likely espionage campaign.[175] The group operated in environments where a common enterprise resource planning (ERP) system[u] was present, raising the possibility that a supply chain compromise served as the initial access vector.
- Between 2023 and early 2025, **Lotus Blossom** conducted cyber espionage operations against Taiwanese government agencies, telecommunications providers, manufacturers, and media organizations. Similar targets in Hong Kong, the Philippines, and Vietnam, also part of the PRC's strategic periphery, were affected as well.[176]

[t] The precise meaning of “cyberattacks” in the NSB’s figures is unclear.

[u] **Enterprise resource planning (ERP) systems** are integrated software platforms used to manage core business functions, such as finance, supply chain, manufacturing, and human resources, through a centralized and trusted IT environment.

South China Sea

Beijing is using cyber and influence operations to weaken Philippine maritime resistance and constrain U.S.-aligned coordination in the South China Sea. Recent activity reflects a dual intent: to penetrate the institutions most relevant to sovereignty enforcement, and to shape perceptions about the legitimacy, capacity, and independence of those institutions. The focus on maritime enforcement infrastructure coincides with political inflection points and coordinated PRC state media messaging. This pattern suggests a strategic goal to degrade both domestic consensus and international partnerships that could challenge PRC maritime expansion. These activities reinforce a broader pattern of calibrated coercion that fuses digital intrusions with political messaging to erode alignment among regional claimants.

- Over five days in August 2023, **Stately Taurus** compromised Philippine government infrastructure as part of a cyber espionage campaign. The campaign coincided with a major maritime standoff between Manila and Beijing in the South China Sea:[177] A high-profile confrontation at Second Thomas Shoal, in which Philippine supply boats breached a PRC coast guard blockade to reinforce a military outpost.[178] The timing suggests the intrusions were intended to collect sensitive information on Philippine decision-making, deployments, or coordination with U.S. forces amid this escalating regional crisis.
- From early 2024 through June 2024, PRC operators, possibly linked to **APT41**, conducted a prolonged espionage campaign targeting multiple Philippine government entities, including the Philippine Department of Information and Communications Technology (DICT),[179] the National Coast Watch Center, and hospital networks.[180] Stolen materials included sensitive military documents, some related to the South China Sea dispute.
- During this same period, the Philippine Coast Guard was a persistent target of cyber operations, with attribution pointing to operators using PRC-based infrastructure.[181] In January, Philippine officials reported intrusions affecting the Coast Guard's website, the website of President Marcos Jr., and the National Coast Watch Center. In February, the Coast Guard's official account on X (formerly Twitter) was compromised, followed by a March 29 hijacking of its official Facebook page, where unauthorized actors posted short-form propaganda videos before access was restored six days later. While limited to public-facing platforms, the operation likely aimed to influence perceptions of an agency central to Manila's maritime enforcement posture.
- In July 2024, a deepfake video falsely portraying Philippine President Ferdinand Marcos Jr. as using illicit drugs was circulated online by an opposition-aligned activist and later amplified by **Spamouflage.**[182] The video was disseminated just hours before Marcos's state of the nation address and appeared intended to inflame political divisions, particularly among supporters of former president Rodrigo Duterte. The operation coincided with a broader shift in Marcos's posture toward a more assertive resistance to PRC activities in the South China Sea.
- The operations during this period prompted direct outreach by the government of the Philippines to foreign cybersecurity partners, including the U.S., Japan, Australia, and the UK. PRC state media and affiliated analysts rejected the attribution to the PRC as technically unsubstantiated, framing it as part of a U.S.-orchestrated "gray zone" cognitive warfare campaign intended to stir tensions and draw Manila closer to Washington.[183]

PRC operations in Vietnam and the Philippines appear designed to maximize visibility into terrain, infrastructure, and national decision-making relevant to a South China Sea crisis. Activity since 2021 reflects a blend of cyber intrusion, physical reconnaissance, and human-enabled collection aimed at systems that would be central to civil and military mobilization during regional escalation. These campaigns likely serve overlapping purposes: long-term intelligence gathering, preparation for contingency operations, and monitoring of sectors that could influence regional alignment. While disruptive capability is not clearly demonstrated, the targets, which include air-gapped systems, critical infrastructure, and strategic terrain, suggest a posture oriented toward access, understanding, and creating options for Beijing.

- Between late 2021 and 2022, **UNC4191** conducted a cyber espionage campaign using self-replicating malware designed to reach air-gapped systems via infected USB thumb drives.[184] While victims were located globally, the campaign disproportionately affected systems physically located in the Philippines, suggesting a deliberate effort to extract intelligence or develop access from hardened sites in the country.

- From 2021 to 2024, a PRC national operating under journalistic cover in Manila developed a human contact network across Philippine government, media, academia, and critical infrastructure sectors, including energy.[185] Philippine intelligence identified the individual as an agent of the **MSS** and cited regular embassy contact, engagements with Huawei and Hikvision officials, and efforts to facilitate deeper integration of PRC technology into public institutions.
- In early 2023, **Earth Longzhi**, a subgroup of **APT41**, targeted government, healthcare, manufacturing, and technology entities in the Philippines, Taiwan, Thailand, and Fiji.[186] Additional decoy documents in Vietnamese and Indonesian point to possible targeting in those countries as well. While the group is known to blend espionage and financially motivated operations, the regional breadth and institutional targeting in this spearphishing campaign suggest a primary focus on strategic intelligence collection.
- In January 2025, Philippine authorities arrested a software engineer from the PRC and two Philippine nationals on espionage charges for conducting unauthorized intelligence, surveillance, and reconnaissance (ISR) operations targeting critical infrastructure across Luzon.[187] The primary suspect, a graduate of the PLA University of Science and Technology, operated a vehicle outfitted with surveillance and remote-access technology to map terrain and strategic sites over the previous month. The operation was allegedly financed by a PRC-based coordinator, who arranged equipment acquisition and oversaw logistical support from abroad.

Japan

PRC operators are targeting Japan's advanced technology ecosystem to accelerate domestic innovation and reduce strategic dependency. A growing share of PRC cyber espionage against Japan focuses on industrial, materials, and energy sectors central to next-generation technological development. The targeting is tightly aligned with Beijing's dual priorities of strategic self-sufficiency and economic competitiveness. These operations appear designed to steal proprietary knowledge from Japan's technology research and high-value manufacturing ecosystems, particularly in areas like semiconductors, aerospace, and telecommunications.

- From 2019 through at least mid-2024, **MirrorFace** conducted over 200 cyber espionage operations targeting diverse Japanese entities.[188][189][190] Starting around 2023, the group expanded its operations beyond earlier political and media targets to manufacturing and research institutions.[191] The new targets included research institutions and private firms in strategic sectors including semiconductors, aerospace, telecommunications, and advanced manufacturing.[192] Japanese authorities assessed the activity as a state-directed campaign linked to the **MSS**, intended to collect intelligence related to national security and advanced technologies.
- In early 2024, **APT41** conducted an espionage campaign targeting Japanese manufacturing, materials, and energy firms.[193] The adversary abused shared access credentials used by third-party maintenance providers to pivot into multiple organizations.

PRC cyber operators appear to be embedding in Japanese critical infrastructure to support contingency operations in the event of regional crises. Recent campaigns have emphasized long-term access to energy, telecommunications, and defense-adjacent sectors, networks that would be critical in a conflict or crisis. While some access may support espionage or early warning, the tradecraft and targeting suggest an intent to prepare for disruption, impose friction, and hold key systems at risk during escalation.

- In 2023, **BlackTech** compromised edge routers at overseas subsidiaries of Japanese and U.S. firms and then exploited trusted network relationships to pivot into parent company networks.[194] The joint U.S.-Japan alert on this activity noted that the group has historically targeted government, industrial, technology, media, electronics, and telecommunications organizations and drew attention to its targeting of entities supporting the U.S. and Japanese militaries.
- Since at least 2023, PRC-linked actors, using what JPCERT called "**Volt Typhoon**-like" tactics, have sought persistent access to Japanese energy, transportation, water, telecommunications, and defense-related research sectors.[195] JPCERT assessed that the objective was to establish access for potential future disruption during crises, rather than immediate data theft or espionage. The activity is tracked as **Operation Blotless**, likely referring to the group's use of living off the land techniques, which JPCERT noted was similar to Volt Typhoon.[196]

PRC cyber operators are surveilling Japanese national security and foreign policy institutions, likely to inform assessments of Tokyo's strategic alignment and alliance behavior. Campaigns since 2022 have included access operations against Cabinet-level cybersecurity bodies, political think tanks, and media platforms, suggesting an effort to collect insight into Japan's evolving role in Indo-Pacific security. While some targets may also serve broader intelligence priorities, the tradecraft and timing point to a focused interest in alliance coordination, policy formulation, and elite decision-making.

- Starting around June 2024 and continuing through at least October 2024, **Earth Kasha**, which is part of **APT10**, conducted a spear-phishing campaign targeting individuals in Japan associated with political organizations, think tanks, and international affairs institutions.[197] The lures referenced topics such as interview requests, U.S.-China relations, and directories of government agencies, suggesting a focus on Japan's national security and foreign policy posture.
- A watering hole campaign in 2023 compromised a Japanese media-related website to deliver targeted malware.[198] Although attribution was unclear, JPCERT noted parallels to **APT10** tradecraft, suggesting ongoing interest in surveillance of Japan's information environment.
- Since 2019 and continuing into 2025, **MirrorFace** has persistently conducted operations against Japanese political and media institutions.[199] This sustained focus highlights the importance of elite perception management and policy surveillance to PRC collection priorities.
- Between October 2022 and June 2023, **UNC4841**[200] compromised Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) by exploiting a zero-day in Barracuda Email Security Gateway appliances,[201] enabling access to internal email accounts and sensitive Cabinet Office communications. The intrusion went undetected for nine months, raising concerns about potential lateral movement and the exposure of allied defense coordination amid expanding Japan-U.S. cyber cooperation.[202]

Eroding Cohesion of the U.S. Alliance System

Beijing is targeting the backbone of the U.S. alliance system, recognizing both its enduring strategic importance and its growing vulnerability. Across Continental Europe and the Five Eyes,[v] political fragmentation, leadership turnover, recalibrated security priorities, and divergent threat perceptions are creating openings that the PRC is systematically exploiting. PRC operations prioritize embedding technical and political access into decision-making ecosystems, shaping elite discourse, and eroding cohesion from within.

This strategy reflects a deliberate effort to treat alliance resilience as a contested arena, targeting the political, economic, and informational seams where collective action is negotiated. While many of these fractures stem from internal frictions among allies, Beijing's activities amplify them, compounding doubts about the reliability, agility, and long-term alignment of U.S.-oriented coalitions.[203] [204] [205] If left unchecked, these operations risk hollowing the foundations of allied coordination, delaying crisis response, and creating structural inertia against policy shifts that would otherwise counter PRC strategic gains. Over time, the cumulative effect could leave U.S.-aligned coalitions slower, more divided, and less capable of adapting cohesively to geopolitical competition, ceding critical ground to Beijing without open confrontation.

Continental European Allies

Since 2022, Beijing has intensified cyber espionage against European diplomatic and government institutions to monitor how the region is adjusting its foreign policy in response to the Russia-Ukraine war. These campaigns have focused on tracking positions on sanctions, defense cooperation, and evolving diplomatic alignments, particularly where they intersect with Taiwan. The activity suggests a PRC concern that the war is accelerating shifts in regional threat perception, weakening Beijing's diplomatic leverage, and expanding political space in Europe for closer engagement with Taipei.

- Between early 2022 and mid 2023, **Mustang Panda** conducted an espionage campaign targeting European government and diplomatic entities using lures referencing NATO, E.U. sanctions, border security, and strategic defense cooperation.[206] [207] [208] [209] [210] The group's phishing often used policy documents tied to the Ukraine war, such as energy sanctions. While most operations appeared geographically dispersed, suggesting broad intelligence gathering efforts, others reportedly narrowly targeted specific regions, such as targeted foreign ministries and embassies across Eastern Europe.[211]
- Between early 2022 and at least April 2023, **APT15** maintained persistent access to Slovenia's Ministry of Foreign and European Affairs, likely to monitor shifts in the country's policy toward the PRC and Taiwan.[212] Slovenian officials linked the intrusion to Prime Minister Janša's early 2022 remarks in support of closer ties with Taipei.[213] Investigators reported that the breach exposed sensitive diplomatic communications, including exchanges with other European foreign ministries, suggesting broader regional surveillance tied to evolving European alignment on cross-Strait issues.
- Between mid-2023 and 2024, **SneakyChef** similarly targeted European government entities using phishing lures impersonating Latvian and Lithuanian foreign ministries, plausibly to monitor growing Baltic engagement with Taiwan.[214] The campaign coincided with a diplomatic tour by Taiwan's foreign minister and a series of parliamentary visits and policy statements strengthening ties with Taipei.[215] These moves reflected a broader realignment triggered by the Ukraine war, which deepened Baltic threat perceptions of authoritarian alignment, which elevated Taiwan as a symbolic counterpoint to PRC-Russian cooperation. The operation suggests PRC interest in how the war has reshaped diplomatic space in Europe in ways that weaken Beijing's influence and legitimize closer Taiwan engagement.
- In August 2024, **Mustang Panda** likely targeted attendees or prospective attendees of the IISS Defence (sic) Summit[w] in Prague using an event agenda lure. The 2024 summit's focus on European defense procurement, technology collaboration, and alliance readiness likely drew PRC interest in monitoring evolving NATO posture, emerging defense partnerships, and long-term defense planning.[216]

[v] **The Five Eyes** is an intelligence-sharing alliance among the U.S., United Kingdom, Canada, Australia, and New Zealand. While not a military alliance, it reflects some of the U.S.'s deepest security, intelligence, and strategic relationships, shaping coordination across defense, technology, and national security domains.

[w] **The IISS Defence Summit** is a high-level forum convened by the International Institute for Strategic Studies to advance Euro-Atlantic defense cooperation, bringing together political, military, and industry leaders to translate policy goals into practical steps for capability development, innovation, and strategic coordination.

The PRC's cyber and influence operations against Italy intensified as the once-symbolic partnership between the two countries unraveled between 2022 and 2024. In 2019, Italy became the only G7 country to formally join the BRI. Beijing heralded the move as a diplomatic breakthrough into highly developed countries.[217] But the relationship never delivered the economic dividends Italy had hoped for. As geopolitical tensions rose over the PRC's support for Russia and concerns about economic coercion, Rome moved to unwind the agreement.[218] Italy's formal exit from the BRI in late 2023 marked a broader strategic realignment: toward closer transatlantic coordination and away from PRC-backed infrastructure and trade frameworks. In parallel, PRC-linked cyber actors launched a series of espionage, access, and influence operations targeting Italian government, industrial, and information ecosystems. These campaigns suggest that Beijing viewed the breakdown of this major BRI relationship both as a diplomatic loss and a risk to be managed through persistent monitoring, technical penetration, and narrative control.

- Between late 2022 and 2024, **APT41** and affiliated actors like **Earth Baku** expanded espionage operations against Italian government,[219] industrial,[220] and logistics[221] sectors amid deteriorating bilateral ties. This included long-term access to an Italian industrial firm in the summer of 2023 during a period of heightened scrutiny over foreign investment and technology exposure, reflecting sustained interest in sectors central to Italy's economic security posture.[222]
- In August and September 2024, **APT41** included Italy in a phishing campaign impersonating tax authorities across NATO and E.U. countries.[223] Italy's inclusion, alongside traditionally high-priority targets like France and Germany, suggests it was being treated as part of Beijing's core surveillance pool following its formal exit from the BRI and deepening realignment with the transatlantic security order.
- In October 2023, a network of fake Italian-language websites was uncovered promoting pro-PRC narratives under the guise of legitimate news outlets.[224] [225] The sites republished unattributed PRC state content and framed Western foreign policy as destabilizing. Their appearance shortly before Italy's BRI withdrawal suggests an effort to influence domestic opinion or mitigate reputational costs as the bilateral relationship fractured.

Beijing's cyber operations maintain persistent access to Europe's defense-industrial base as the continent slowly reorients its security posture. This activity coincides with a mounting European reassessment of economic and technology dependencies on the PRC, especially in Germany, where increasing political skepticism of Beijing and military aid to Ukraine are reshaping procurement and policy.[226] Beijing appears intent on preserving insight into European rearmament trajectories and hedging against future restrictions that may constrain its strategic reach.

- In April 2024, German authorities arrested three individuals accused of acquiring military-use technologies for the **MSS.**[227] Operating through a front company, the group allegedly worked with German research institutions to obtain sensitive designs, including naval engine technology, and was negotiating further projects linked to the PRC's naval buildup. Authorities also charged the suspects with illegally exporting a restricted laser system in violation of E.U. dual-use controls. The arrests came one week after then-Chancellor Olaf Scholz raised concerns in Beijing over PRC acquisition of dual-use technologies and support for Russia's war effort.[228]
- Throughout 2023 and 2024, **Earth Estries** conducted sustained cyber espionage operations with confirmed targeting in Germany and a probable focus on government and technology sectors.[229]
- In early 2024, **Mustang Panda** targeted cargo shipping firms in Norway, Greece, and the Netherlands, placing malware on corporate networks and vessel-based systems.[230] Its targeting of Europe's maritime transportation sector continued into 2025.[231] A similar 2022 incident saw PRC-linked malware discovered aboard seven vessels from a single fleet, where it had likely persisted undetected for up to two years, underscoring PRC interest in onboard systems as a persistent access vector.[232] Together, these cases suggest sustained PRC interest in maritime infrastructure, offering insights into trade flows, vessel movements, and defense logistics.[233]
- As of mid-2023, encrypted storage devices used by NATO and the UK Ministry of Defence (sic) still contained chips made by a PLA-linked company.[234] [235] While not tied to a specific operation, the finding underscores the enduring risk posed by PRC-made components embedded in Western defense systems and highlights the need for long-term efforts to secure supply chains.

Five Eyes Allies

Beijing is seeking to shape the political environment of the United States' Five Eyes allies in its favor. It aims to influence political discourse and perceptions, undermine critics while promoting aligned actors, and erode trust in institutions and alliances. In parallel, it collects intelligence on key political figures and institutions to inform Beijing's diplomatic and commercial positioning and to steer policy alignment in its favor. These efforts seek to constrain policies adverse to PRC interests, promote more accommodating foreign policy positions, and weaken cohesion among U.S. allies. Publicly available information about these campaigns reflects efforts to influence political dynamics without directly disrupting electoral processes or infrastructure.

- In the lead-up to Canada's 2025 federal election, PRC-aligned influence campaigns targeted ethnically Chinese voters with messaging portraying the Conservative Party as hostile to PRC interests and a threat to diaspora communities.[236] [237] These narratives echoed tactics the PRC[238] used in 2019 and 2021 to marginalize Beijing's critics in Canada. At the same time, PRC state media favorably framed then-candidate and eventual-winner Liberal Party leader Mark Carney as a pragmatic figure who might stabilize bilateral ties, even after he publicly labeled the PRC Canada's "biggest security threat."[239] [240]
- From 2023 to 2025, PRC-linked information operations in Australia amplified narratives favorable to the ruling Labor Party while casting Opposition Leader Peter Dutton as a destabilizing, U.S.-aligned figure likely to provoke confrontation and economic harm.[241] [242] Inauthentic accounts spread divisive content across Western and PRC platforms, stoking domestic tension around race, gender, and economic inequality. These accounts positioned Labor as the more pragmatic steward of bilateral ties, while the AUKUS[x] pact and Australian intelligence services were framed as vectors of foreign control.
- In August and September 2023, **Spamouflage** coordinated multilingual malign influence content across a dozen platforms and at least 15 languages targeting Canada, the U.K., and the U.S. The campaign amplified a fabricated narrative blaming the Maui wildfires on a U.S. "weather weapon," citing a fictitious British intelligence leak.[243] It used social media accounts to harass Canadian Prime Minister Justin Trudeau and other officials with deepfakes, criminal accusations, and conspiratorial content.[244] The operation appeared designed to degrade trust in Western leadership and create fractures among Five Eyes governments.
- In March 2024, the UK publicly attributed two cyber operations to PRC state-affiliated actors. Authorities assessed that an unspecified group had compromised Electoral Commission systems between late 2021 and October 2022, stealing voter registration data. No impact on electoral processes was reported.[245] The government also assessed that **APT31** conducted reconnaissance against Members of Parliament critical of Beijing in 2021.[246] In response, the UK sanctioned two APT31 members and a front company linked to the MSS.
- In 2024, New Zealand attributed two prior cyber operations to PRC-linked groups. In March, the government assessed that **APT40** was responsible for a 2021 intrusion into the Parliamentary Counsel Office and Parliamentary Services.[247] In April, the country's national signals intelligence agency revealed that **APT31** had targeted former Members of Parliament and an academic affiliated with the Inter-Parliamentary Alliance on China. Both operations appeared intended to monitor and potentially deter elite political criticism of the PRC.[248]
- In early 2025, Canadian authorities announced that they had attributed over 20 recent PRC-linked intrusions targeting all levels of government. Officials assessed the activity aimed to collect political, economic, and personal data to support Beijing's commercial and diplomatic positioning, particularly in areas related to energy, critical minerals, and regional trade.[249]

[x] **AUKUS** is a security partnership between Australia, the United Kingdom, and the United States focused on Indo-Pacific stability and security.

Beijing is targeting the defense and critical infrastructure ecosystems of the U.S.'s Five Eyes allies to gain access, collect information, and prepare for future contingencies. The targeting pattern suggests a priority on mapping defense institutions, monitoring activity, and establishing persistent access that could support espionage or disruption if needed.

- In 2024, UK officials assessed that PRC-linked operators, possibly including **Volt Typhoon**, had likely maintained persistent access to numerous important domestic networks for years.[250] The activity reportedly affected defense, energy, healthcare (including the National Health Service), government, high-tech firms, and senior politicians' communications. Officials noted compromises of both supply chains and systems underpinning essential services.
- In April 2025, Canadian authorities warned that PRC threat actors, including **Salt Typhoon**, had repeatedly exploited vulnerable edge routers across critical infrastructure sectors.[251] The actors exploited weak credentials, altered settings for persistence, and exfiltrated device configurations to support further access.
- Since at least 2022, PRC actors, including **Volt Typhoon**, have operated a botnet built from compromised end-of-life routers to enable espionage and prepositioning against the U.S. and its Five Eyes partners. U.S. authorities disrupted part of the botnet in early 2024, which had been used to support intrusions into the country's critical infrastructure.[252] Associated traffic included connections to U.S., UK, and Australian government domains, indicating likely reconnaissance or access staging.[253] [254] [255]
- In May 2024, UK officials disclosed that a suspected PRC-linked group breached a Ministry of Defence (sic) payroll system, compromising sensitive personal and financial data tied to personnel across the Royal Navy, Army, and Royal Air Force.[256] While not formally attributed, officials stated the activity resembled known PRC-linked operations.
- Between late 2023 and early 2024, **UNC5174** exploited vulnerabilities in widely deployed network management tools to access government and defense-related systems in the UK, Canada, and U.S.[257] The actor established persistent backdoor access, conducted internal reconnaissance, and targeted national security entities, including U.S. defense contractors and UK government networks.

Locking in Leverage in Developing Countries

The PRC views the developing countries that lie outside U.S.-aligned security and economic systems as a strategic operating space where it can expand influence with minimal resistance and maximal return. These regions, often highly receptive to infrastructure-backed engagement, provide low-friction environments for shaping political orientation, embedding technical dependencies, and constraining external actors. Cyber operations support these efforts by securing access to government systems, critical infrastructure, and regional communications platforms that the PRC has helped build or finance. Information campaigns run in parallel, reinforcing preferred narratives, deflecting scrutiny, and undermining confidence in alternative governance models. Together, these operations are steadily positioning Beijing as an embedded, often unconstrained external actor in regions whose future alignment will shape global strategic outcomes.[258] [259]

Recent PRC cyber and influence campaigns across the developing world show the PRC attempting to shape diplomatic alignment, monitor political developments, and constrain external influence. These operations provide access to elite decision-making and create leverage over governments that rely on PRC-built infrastructure, particularly in moments of political uncertainty or negotiation. By embedding in the digital systems and media environments of these countries, Beijing is reducing the maneuvering space of competitors and conditioning regional actors to treat PRC preferences as default constraints. Left unchecked, this trend risks ceding informational and technical ground in strategically located countries where Beijing is well positioned to preempt external basing, limit U.S. bilateral access, and top the balance in long-term regional influence contests.

Africa

Beijing's cyber operations in Africa appear calibrated to manage political and economic risk in countries where the PRC maintains expanding strategic investments or diplomatic footholds. Since 2022, PRC-linked actors have targeted government institutions and elite decision-making bodies in countries where policy or leadership changes could affect long-term PRC interests. These efforts are especially concentrated in BRI partner countries and regions where PRC-backed infrastructure projects have generated financial or political friction.

- Reporting in 2023 noted that **BackdoorDiplomacy** had maintained multi-year access to at least eight Kenyan government entities, including the ministries of finance and foreign affairs and the National Intelligence Service. This access likely supported monitoring of debt repayment, elite alignment, and policy shifts affecting PRC infrastructure projects as financial strain mounted.[260]
- In 2024, **RedDelta** conducted espionage against Ethiopian government institutions,[261] shortly after the country signed a new strategic cooperation agreement with Beijing.[262] The operation possibly served to monitor the implementation of this bilateral initiative or related internal political dynamics.
- In 2024, **IcePeony** targeted Mauritian government entities[263] amid deepening defense and economic ties with India[264] and negotiations with Britain over transferring the disputed Chagos Islands.
- In 2024, researchers identified a novel PRC-linked malware framework dubbed IMEEX targeting systems in Djibouti. While the campaign's exact objectives were not determined, the use of a custom modular backdoor in such a geopolitically sensitive state points to an interest in maintaining persistent access aligned with Beijing's regional strategic equities. In possibly relevant context, Djibouti is home to the PLA's only overseas base as well as ones belonging to the United States, France, and Japan.[265]
- In 2025, **SneakyChef** likely compromised Angolan foreign affairs and development institutions[266] during an uptick in PRC engagement, coinciding with renewed infrastructure deals in a major investment and resource partner.[267]

PRC cyber operations also prioritize strategic positioning within African telecommunications infrastructure to maintain access, collect sensitive data, and reinforce technical dependency. These efforts target both core telecom providers and the supporting vendor ecosystems that maintain or operate PRC-built platforms across the continent.

- Around 2021, **Liminal Panda** developed tooling tailored to mobile network protocols, including GSM emulation and SIGTRAN abuse, with activity documented in Africa.[268]
- Around 2023 to 2024, **Earth Estries** compromised South African telecom providers and third-party firms responsible for maintaining PRC-linked infrastructure, indicating an interest in long-term visibility into regional telecom operations.[269]
- In approximately early 2023, **Mustang Panda** deployed USB-based malware in Ghana and Nigeria, likely designed to reach air-gapped or lightly monitored systems embedded in national telecom and government networks.[270]
- Between at least late 2022 and early 2023, **Daggerfly** compromised African telecom networks using modular malware, with capabilities for credential harvesting, audio capture, and internal reconnaissance.[271]
- In early 2023, PRC-linked actors behind **Operation Tainted Love** compromised a North African telecommunications firm during a period of regional expansion negotiations. The timing suggests the operation was intended to gather internal business intelligence, support diplomatic leverage, or maintain long-term technical access aligned with Beijing's soft power interests.[272]

Beijing's information operations in Africa complement its cyber campaigns by shaping public perception, amplifying pro-PRC narratives, and diluting or discrediting competing perspectives. These efforts rely on infrastructure that conceals state involvement, using pseudo-local voices to insert Beijing's messaging into African political discourse.

- Since 2022, PRC-linked digital marketing firms operating under the **GLASSBRIDGE** umbrella have run networks of inauthentic news websites across Africa and other regions. These sites mimic legitimate local outlets while promoting pro-Beijing narratives, often republishing PRC state media content and distributing it via commercial newswire services to create the appearance of credible, locally sourced journalism.[273]
- In 2023, Meta removed thousands of fake Facebook and Instagram accounts linked to PRC actors, which posed as African users and media brands.[274] These accounts promoted Beijing as a reliable development partner, praised BRI projects in Kenya and Nigeria, and portrayed Western engagement as destabilizing or neocolonial. Some repurposed anti-dissident propaganda for African audiences, blending global messaging with localized influence goals.

Latin America

Beijing's cyber and influence operations in Latin America are primarily designed to preserve and protect its expanding economic and diplomatic footprint across the region. The PRC is now the top trading partner for much of Latin America and exerts growing control over key logistics hubs and diplomatic footholds.[275] Activity in 2023–2024 has been especially concentrated in countries with major PRC investments or where volatile public sentiment could threaten Beijing's long-term leverage. This activity challenges longstanding U.S. leadership in the hemisphere and signals Beijing's intent to shape regional alignments in ways that may constrain U.S. strategic access and policy leverage.

- Active since at least 2022, **Operation LongFang** has targeted municipal governments and critical infrastructure sectors across Latin America, with a concentration in Brazil. The operation focuses on collecting government records, infrastructure blueprints, and urban planning documents.[276] Meanwhile, **Earth Estries** targeted Brazilian logistics and telecommunications firms, sectors closely aligned with PRC infrastructure investment.[277]

- Also in Brazil, PRC-linked influence networks **PAPERWALL**[278] and **GLASSBRIDGE**[279] disseminated Beijing-aligned narratives, via spoofed or co-opted local media channels, often focusing on politically sensitive themes.

- In recent years, several PRC cyber espionage groups previously focused on East Asia have expanded into Latin America. Since March 2023, PRC-aligned threat cluster **CL-STA-0049** has targeted government, defense, telecommunications, and aviation sectors in South America alongside its Southeast Asia target-set.[280] In mid-2024, **Earth Alux** extended operations into Latin America —particularly in Brazil—with a focus on government, logistics, telecommunications, and IT services.[281] Also in 2024, **Sharp Dragon** began targeting Caribbean and African government entities using diplomatic-themed lures and previously compromised Southeast Asian infrastructure.[282]

- In 2024, **FamousSparrow**, a group overlapping with **Earth Estries**, compromised a research institute in Mexico, a government entity in Honduras, and a U.S. trade group. The Honduras activity followed the country's 2023 diplomatic shift from Taipei to Beijing, possibly reflecting PRC interest in shaping or monitoring early bilateral engagement and reputational dynamics post-switch.[283]

- Between late 2022 and early 2023, **APT15** targeted a business operating across Central and South America, along with regional foreign affairs and finance ministries, suggesting interest in commercial networks and diplomatic posture.[284]

- In 2024, the U.S. and Costa Rica jointly announced that PRC-based adversaries had infiltrated Costa Rican telecommunications and technology systems. Though they did not explicitly attribute the operation to the PRC government, the U.S. reaffirmed its support for Costa Rica's sovereignty, a possible diplomatic signal of suspected state involvement.[285] The announcement followed Costa Rica's 2023 decision to exclude PRC technology firms from its 5G network rollout due to cybersecurity concerns.[286]

Beijing's cyber and influence operations in Latin America also target many of Taiwan's remaining diplomatic footholds by shaping domestic environments to deter recognition or reduce resistance to Beijing's position. Since 2017, broader pressure campaigns have led four countries—Panama, the Dominican Republic, El Salvador, and Honduras—to sever ties with Taipei. Cyber and information operations focus on government institutions and domestic audiences in countries where alignment remains contested, allowing Beijing to suppress dissent and amplify pro-Beijing narratives through deniable means.

- In 2021, Guyana abruptly reversed plans to deepen engagement with Taipei following pressure from Beijing, underscoring the PRC's intolerance for even symbolic gestures toward recognizing Taiwan.[287 288] In early 2022, **Earth Krahang** spearphished regional government entities using Taiwan-related geopolitical lures, likely targeting institutions involved in or adjacent to Taiwan-Guyana relations.[289]
- In September 2022, PRC-linked actors compromised Guatemala's foreign ministry[290] shortly after the country reaffirmed diplomatic ties with Taiwan. Based on the timing, the operation plausibly sought to monitor the countries' bilateral engagement or shape perceptions in one of Taipei's few remaining Central American partners.[291]
- During the 2023 Paraguayan election, a China News Service–linked influence network pushed Beijing-aligned narratives about Taiwan into Spanish and Portuguese-language content targeting voters in Paraguay,[292] the region's most diplomatically significant Taiwan-aligned country.[293]
- In November 2024, a joint cybersecurity review by the U.S. and Paraguay identified **Flax Typhoon** infiltrations into Paraguayan government systems.[294] Paraguay's technology minister described the incident as a "silent vulnerability" aimed at capturing sensitive diplomatic and strategic communications, with the potential to compromise the country's "operability and international relations."[295]

Pacific Islands

Beijing's cyber and influence operations in the Pacific Islands aim to weaken U.S. strategic footholds, disrupt trusted multilateral processes, and shift regional alignment through persistent, low-cost interference. Since 2022, the PRC has exploited the limited cyber resilience and institutional capacity of Pacific Island governments to collect intelligence, shape elite narratives, and obstruct U.S.-backed coordination efforts. These operations target environments where even minor compromises threaten to yield outsized geopolitical returns:[296] [297] undermining U.S. basing arrangements, eroding diplomatic trust, and tilting votes in international bodies where every state counts equally.[298] The pattern reflects a deliberate effort to turn vulnerability into leverage in a region critical to forward U.S. power projection and alliance credibility.[299]

- In early 2024, PRC state-backed actors reportedly infiltrated the Pacific Islands Forum Secretariat in Fiji. Australian officials described the campaign as "extensive" and aimed at accessing and assessing internal diplomatic coordination.[300]
- In that same month, a ransomware attack on Palau leaked thousands of documents, including internal U.S. defense planning and Palau-Taiwan coordination. Palau hosts critical U.S. military access agreements and is a formal Taiwan partner.[301] Ransom links were nonfunctional, suggesting a political objective rather than a financial one. The content and concurrent timing with a high-profile U.S.-Palau compact ceremony[y] point to a likely effort to signal displeasure with Palau's trilateral relationship with Taipei and Washington. Palau's president noted that the "attack likely originated from Malaysia with Chinese or Russian ties."[302]
- In the run-up to the Solomon Islands' 2024 election, PRC and Russian state media amplified engineered narratives accusing the U.S. of planning to interfere in the country's affairs.[303]
- In February 2025, Samoa's national cyber agency reported that **APT40** had specifically compromised networks across the Pacific Islands.[304] The group reportedly maintained long-term persistence before exfiltrating data. Samoa did not specify which organizations were impacted, but generally noted the group's historic targeting of government and critical infrastructure organizations.

Beijing also appears to be using cyber operations to expose, disrupt, or delegitimize Taiwan's remaining diplomatic footholds in the Pacific.

These activities reflect a broader strategy of information collection, reputational targeting, and influence over political narratives in countries that still formally recognize Taipei. PRC-linked actors appear particularly focused on mapping Taiwan's modes of international engagement and using public exposure to erode their perceived legitimacy.

- The 2024 Palau ransomware operation leaked internal records detailing Taiwanese funding for Palau's participation in global forums, including UN climate summits, potentially exposing Taipei's mechanisms for sustaining diplomatic visibility.[305]
- The 2024 Solomon Islands influence campaign drove CCP-aligned narratives, alleging U.S. and Taiwanese retaliatory instigation of riots following the country's diplomatic switch from Taipei to Beijing.[306]

[y] In May 2023, the United States and Palau signed a **renewed funding and defense agreement** under the Compact of Free Association, reinforcing U.S. military access and long-term support for Palau. The deal, concluded amid growing regional tensions, underscored Palau's strategic importance as both a U.S. ally and one of the few nations maintaining formal ties with Taiwan.

Forecasting

6

Forecasting

The following section outlines likely future trajectories in PRC cyber and influence operations based on observed trends and evolving geopolitical and systemic technical conditions. Each forecast highlights how the PRC's existing capabilities and behaviors may scale, adapt, or converge in service of broader strategic objectives. Rather than offering speculative scenarios, these assessments identify directional shifts already in motion: from access to leverage, from denial to contestation, and from surveillance to shaping. Each forecast includes observable indicators to monitor for that would validate these projections, supporting early warning, policy planning, and defensive preparation.

Trusted Access Abuse Scales Up with Persistent Operational Infrastructure

PRC cyber operators will expand how they abuse trusted relationships as both access points and persistent operational footholds. As perimeter defenses improve in response to the network edge device exploitation trend and direct exploitation becomes costlier, leveraging existing structural trust will remain a low-friction, scalable means of compromise. This is especially true for vendor-administered support channels and locally dominant or PRC-developed software platforms. Rather than targeting organizations directly, PRC groups are expected to deepen their focus on third parties already embedded in their targets' infrastructure: managed service providers, upstream platform maintainers, and update distributors with persistent or privileged access.

Operators will refine their use of vendor and supply chain access to better align with mission specificity and operational security. Rather than mass software tampering campaigns, future activity will likely favor tightly scoped, pre-filtered delivery through vendor ecosystems that already serve high-value sectors. PRC actors have demonstrated increasing precision in software delivery operations, embedding targeting logic into the initial deployment phase and minimizing exposure beyond the intended victim set. This shift enables stealthier compromises while maintaining the scale benefits of leveraging centralized access relationships.

Access-as-a-service models will formalize as PRC contractors build infrastructure to exploit or manage trusted relationships at scale. Drawing from prior examples of contractor-managed ORB networks and botnet provisioning, similar models could emerge around vendor access channels, where third-party actors maintain or broker persistent access into vendor environments or update pipelines. This development would reduce operational overhead, create reusable access into diverse customer bases, and provide PRC operators with deniable but durable points of entry into critical sectors.

These trends will converge in politically and industrially strategic geographies, particularly where reliance on PRC-linked service providers remains high and defensive capacity is limited. In such environments, state-aligned operators may not need to breach target systems directly. Instead, they may exploit dependency on regional vendors for software updates, remote support, or hardware servicing. This tactic would likely be especially viable in sectors with delayed patch cycles, weak segmentation, and high third-party integration, including defense, industrial control, telecom, and semiconductor manufacturing.

Potential Key Indicators

Targeting of managed service providers or third-party information technology (IT) support firms across multiple sectors or regions. Evidence that PRC-linked actors are compromising or prepositioning within MSPs, remote support contractors, or cloud service integrators may indicate a continued strategic shift toward scalable indirect access.

Discovery of malware embedded in vendor update infrastructure with constrained, sector-specific delivery. Detection of malware inserted at the software distribution level, particularly when the payload is selectively activated based on sector, geography, or customer profile, may reflect a refined, low-exposure intrusion model.

Emergence of contractor-or state-linked platforms designed to provision, manage, or automate vendor-enabled access. Discovery of infrastructure (e.g., dashboards, APIs, scripting frameworks) built to exploit or control vendor support or update channels, especially from PRC-affiliated firms, would indicate increasing institutionalization of this tactic.

Unexplained overlap across victim organizations linked by shared vendors or support platforms. Targeting clusters in which victims share a common vendor, update mechanism, or administrative tool, without clear strategic or geographic linkage, may signal exploitation of a trusted intermediary.

Exploitation Expands to Nontraditional and Under-Protected Edge Devices

PRC cyber operators will expand their network edge targeting to include other under-monitored infrastructure devices such as satellite terminals,[z] cellular gateways,[aa] and carrier-grade NAT equipment,[bb] particularly in industrial and remote deployments. These devices offer many of the same tactical advantages that have made edge systems central to PRC operations (e.g., limited monitoring, irregular patching, and direct exposure to critical traffic) but are often deployed in environments with even weaker defensive oversight. This potential expansion aligns with the PRC's broader interest in accessing digital infrastructure that supports strategic sectors, including energy, logistics, and military basing.

Operators will also adopt more layered exploitation approaches that combine firmware vulnerabilities with configuration flaws and exposed management interfaces. This reflects a tactical progression already seen in prior campaigns, where PRC actors leveraged both technical exploits and architectural weaknesses to extend access and maintain persistence. Firmware compromise remains especially concerning, as it often enables long-term access that is difficult to detect or remediate, particularly in devices without centralized update mechanisms or endpoint detection and response (EDR) visibility.

Compromised edge devices will be more deliberately integrated into PRC operational infrastructure, serving not just as entry points but as long-term assets for anonymization, command-and-control, and lateral movement. The development of ORB networks and contractor-managed botnets suggests a maturing ecosystem in which infrastructure is provisioned centrally and reused across operations. This infrastructure model reduces cost, complicates attribution, and enables PRC actors to scale access in line with strategic priorities.

These trends are exacerbated by the growing footprint of PRC-manufactured networking hardware in sensitive environments. Even without deliberate compromise, such devices introduce structural exposure, particularly when vulnerability disclosure is governed by PRC regulations that route flaws to state-linked entities. This dynamic increases the likelihood that exploitable weaknesses in globally deployed hardware may be selectively retained for state use, reinforcing Beijing's ability to map and access infrastructure that would otherwise be difficult to compromise through direct means.

[z] **Satellite terminals** provide network connectivity via space-based links, often used in remote or mobile environments with limited monitoring and encryption.

[aa] **Cellular gateways** connect local networks or devices to mobile data networks, often bridging industrial systems to the internet with minimal security controls.

[bb] **Carrier-grade NAT (CGN) equipment**, used by internet service providers (ISPs) to conserve IPv4 addresses, masks individual user activity by routing traffic from many devices through shared public IPs. Adversaries can exploit this to conceal device origins and complicate attribution.

Potential Key Indicators

Increase in PRC technical publications or patent filings focused on industrial edge protocols and emulation: Research into GSM, SCADA, SATCOM, or CGNAT[cc] device emulation, especially from defense-tied institutions or PRC cyber research labs, may reflect tooling preparation or capability incubation.

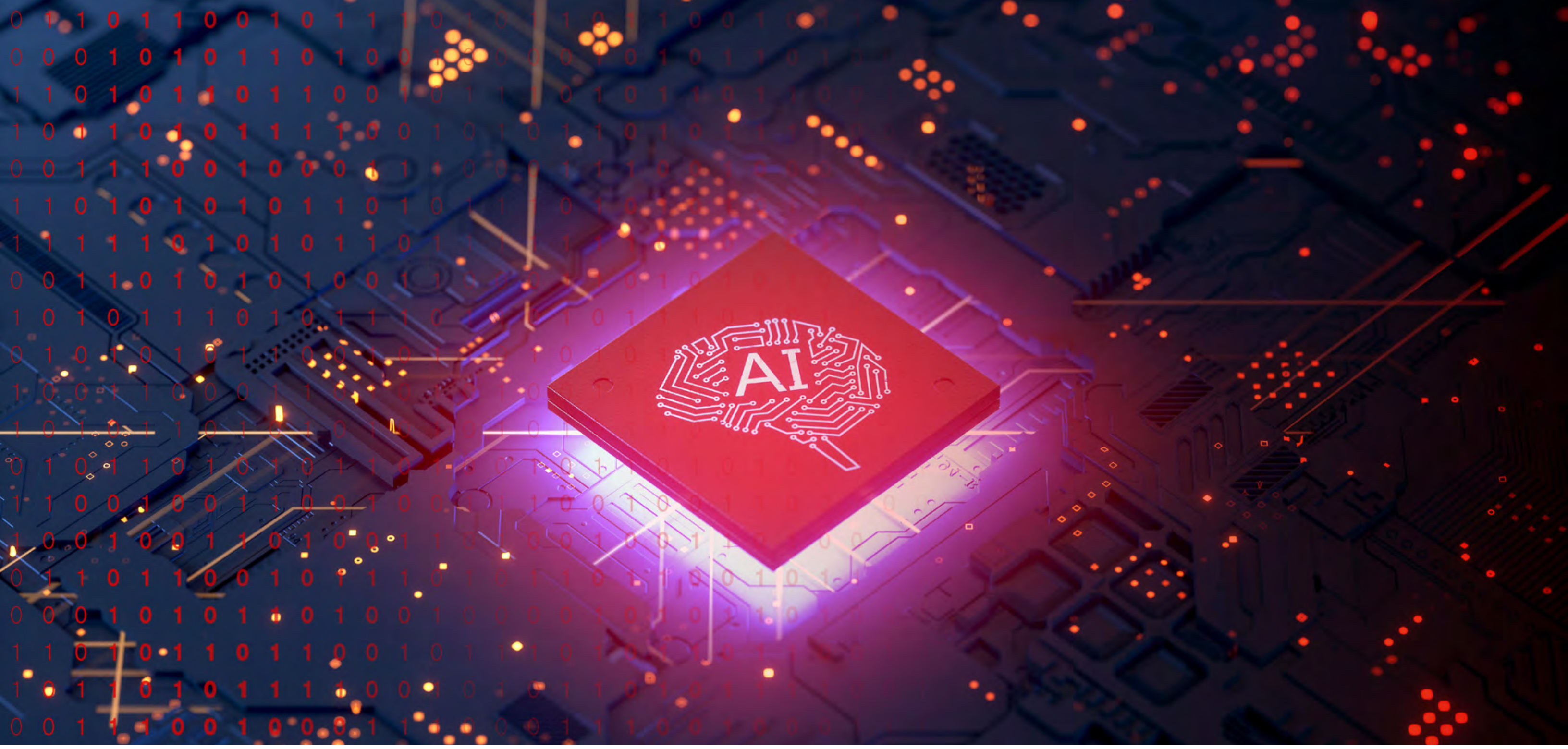
Command-and-control infrastructure built on uncommon edge hardware across multiple regions: Detection of botnet or ORB-like infrastructure using atypical device types (e.g., satellite dishes, LTE gateways) or appearing in multiple geographies aligned with PRC interests suggests a strategic reuse model is maturing.

Emergence of abused vulnerabilities in edge-layer infrastructure not historically targeted. A rise in abused vulnerabilities affecting devices such as satellite modems, cellular gateways, or industrial network equipment may indicate that findings are being withheld for potential operational use. This is particularly likely when these CVEs are not accompanied by public research from PRC sources or disclosure through PRC platforms like CNNVD.[dd]

Public or leaked evidence of contractor-provisioned access to edge-compromised infrastructure. Reporting or disclosures indicating that MSS or PLA-linked firms offer managed access to compromised devices (e.g., via API interfaces, botnet dashboards) would reinforce the forecast of institutionalized infrastructure reuse.

[cc] These are specialized technologies and protocols commonly found in telecommunications and industrial control environments: **GSM** (Global System for Mobile Communications), **SCADA** (Supervisory Control and Data Acquisition), **SATCOM** (Satellite Communications), and **CGNAT** (Carrier-Grade Network Address Translation).

[dd] **China National Vulnerability Database (CNNVD)** is the PRC's national repository for cataloging cybersecurity vulnerabilities.



AI Moves from Support Role to Core Operational Enabler

PRC operators will deepen their integration of AI into cyber espionage and influence operations, extending its role beyond analytic acceleration to support operational scale and prioritization. While current applications focus on processing large datasets and automating content generation, future developments will likely assist human operators in triaging targets, organizing workflows, and coordinating broad digital campaigns. This trajectory reflects Beijing's "intelligentized warfare" doctrine and directly addresses enduring constraints in linguistic reach, analyst throughput, and operator capacity. As AI systems grow more agentic—capable of chaining analytic tasks or autonomously identifying high-value insights—these workflows will become faster, more scalable, and increasingly independent of manual triage.

In cyber operations, AI will be integrated into toolchains that assist with vulnerability analysis, large-scale data parsing, and dynamic target prioritization. These applications would enhance PRC actors' ability to conduct rapid collection campaigns while more efficiently extracting value from diverse, multilingual, and unstructured datasets. While current use cases include malware debugging and translation of technical materials, future developments may support semi-automated scripting or decision-support workflows to reduce operator burden and sustain operations in active defensive environments.

In influence operations, PRC actors will expand the use of AI-enabled systems to generate, tailor, and distribute messaging at scale, with reduced reliance on human operators. PLA writings envision AI-supported psychological operations aimed at exploiting adversary cognitive vulnerabilities, and recent operational errors linked to AI-generated content suggest ongoing experimentation. As capabilities mature, AI may enable real-time generation of synthetic media, automated narrative testing, and more targeted amplification strategies aligned with demographic or linguistic segmentation.

AI integration in PRC operations will accelerate as compute-efficient architectures and lightweight deployment pipelines erode existing technical barriers. Advancements that shrink model sizes, reduce computing demands, and enable local deployment will expand AI adoption. In the near term, applications that demand less compute and carry lower operational risk—such as translation, narrative amplification, or multilingual sentiment analysis—will likely scale fastest. More technically demanding capabilities, such as AI-assisted exploit development or adaptive decision-support tooling, will likely follow as the next major wave.

Potential Key Indicators

Increase in PRC-originating research focused on automating offensive cyber functions with AI. Technical publications or patent filings describing AI-supported vulnerability triage, exploit generation, or targeting workflows, particularly from institutions linked to PLA units, MSS proxies, or defense contractors, may indicate pre-operational capability incubation.

Patent filings or applied research on multilingual sentiment analysis and narrative tailoring from state-aligned institutions. Submissions from organizations affiliated with state media, political warfare programs, or psychological operations that focus on demographic segmentation, sentiment scoring, or generative influence techniques may signal investment in scalable information operations.

Collaboration between political influence researchers and technical AI development labs. Co-authored publications, cross-affiliated lab staff, or joint institutional projects between offensive influence-linked entities and AI modeling teams, especially within national key labs,[ee] may reflect structural alignment of technical and narrative engineering objectives

Targeting of firms or academic institutions with influence-relevant datasets or model control mechanisms. Persistent PRC cyber activity directed at organizations that maintain NLP training corpora,[ff] profiling tools, or research on model guardrail circumvention may indicate an effort to externally source resources that would enhance the adaptability and reach of AI-enabled influence campaigns.

[ee] **National Key Labs** are government-designated research institutions in the PRC that focus on advancing strategic technologies, often in support of national security and economic development goals.

[ff] **NLP corpora** are structured datasets of human language used to train, evaluate, or benchmark natural language processing models.

Plausible Deniability Shifts to Structured Denial Operations

Beijing will develop a faster, more structured playbook for contesting cyber attribution in high-stakes incidents. Recent examples point to more coordinated national messaging around cyber threats. PRC cybersecurity firms, MFA spokespeople, and state media now often issue rebuttals around the same time. This pattern is likely to evolve into a repeatable, more rapid response process. The goal would be to present a unified narrative that quickly challenges the credibility of attribution before a diplomatic consensus can form. Unlike Russia's chaotic response style, which is built on overwhelming and confusing with rapid, conflicting counterclaims, the PRC's approach is already more methodical. It draws on official, commercial, and academic voices to portray attribution as biased or technically flawed. This shift matters. Faster, more coordinated responses would allow Beijing to more credibly shape early perceptions, give neutral countries a reason to stay on the sidelines, and undermine attribution as a basis for joint action. The intent is not to prove innocence, but to delay alignment and weaken the impact of any coordinated response.

Beijing is likely to lean more heavily on criminal or hacktivist proxies in cyber operations where attribution could trigger political fallout or complicate its broader regional ambitions. This is not a new tactic. PRC actors have long used proxy-enabled operations to mask state direction. Still, the logic behind their use is evolving. In areas where escalation is tightly managed and coalition-building poses a growing risk, Beijing is likely to deploy proxies in coercive or disruptive operations that would be politically risky to carry out directly. This shift raises the stakes for cyber leaders: ambiguous campaigns targeting infrastructure, government entities, or civil society may be framed as criminal or rogue acts, delaying coordinated responses and creating friction within alliances. As exposure timelines shrink and diplomatic consequences become more coordinated, proxy-enabled operations allow Beijing to apply pressure while maintaining plausible deniability, blunting policy levers before they can be used.

Potential Key Indicators

Increased technical rigor in attribution rebuttals from PRC cybersecurity firms. Publication of incident reports that replicate reputable cyber threat intelligence's structure may indicate an effort to contest attribution on methodological grounds.

Amplification of attribution rebuttals through semi-academic or state-affiliated research voices. Commentaries, joint reports, or technical articles from PRC think tanks, universities, or affiliated labs that reinforce official attribution counter-narratives may reflect a strategy to diversify the attribution contestation ecosystem while maintaining message discipline.

Disruptive or coercive cyber operations in contested areas with ambiguous operational signatures. Campaigns in Taiwan, the Pacific Islands, or South Asia exhibiting PRC-adjacent infrastructure or tooling but lacking clear espionage or financial motive may indicate proxy-enabled operations calibrated for plausible deniability.

Ransomware or pseudo-criminal operations targeting geopolitical rivals with non-functional extortion mechanisms. Cyber incidents that mimic financially motivated campaigns but show no viable payment infrastructure, no victim negotiation, or incoherent demands may suggest attempts to encourage misattribution of state-backed disruption.

Crisis Delay and Alignment Disruption in the PRC's Strategic Periphery

Cyber prepositioning will complicate crisis response coordination in a future regional contingency. PRC threat actors are establishing persistent access to telecommunications, logistics, and defense-relevant infrastructure in Taiwan and Japan, while also targeting Philippine maritime enforcement systems. If unmitigated, these footholds could delay national response timelines, hinder coordination with US partners and allies, and expose critical systems to disruption in the early stages of escalation. Direct operational use remains unconfirmed in available public sources, but the observed tradecraft and sectoral targeting align with known contingency planning priorities.

Cyber-enabled political warfare threatens to undermine the domestic legitimacy of U.S.-aligned leaders and deter visible forms of alignment. Beijing is intensifying these operations in environments where pro-U.S. stances intersect with electoral vulnerability or contested sovereignty. In Taiwan and the Philippines, manipulative messaging, deepfakes, and amplification campaigns have targeted specific leaders, polarized public opinion, and attempted to erode trust in electoral processes and sovereignty-related enforcement institutions. These tools are likely to be further scaled and tailored, with the support of AI, to exploit domestic fault lines, especially where governments adopt firmer positions against PRC interests.

Sustained cyber espionage targeting U.S. partners' advanced technology sectors risks degrading allied supply chain resilience and accelerating PRC strategic self-sufficiency. PRC cyber operators are systematically extracting proprietary data from semiconductor, aerospace, telecommunications, and manufacturing firms in Taiwan and Japan. These operations align with Beijing's goal of reducing reliance on foreign innovation. If trends continue, this access may accelerate PRC innovation while providing insight into U.S. and allied dependencies on foreign technology suppliers. This insight could inform future disruption or coercion strategies.

Cyber and influence operations will play a persistent role in shaping South China Sea gray-zone confrontations. Future campaigns may increasingly blend observed capabilities spanning cyber intrusions, physical surveillance, human intelligence, and digital influence tactics to manipulate perception, posture, and decision-making below the threshold of armed conflict. Indicators from recent operations in the Philippines suggest that Beijing is refining this toolkit in ways that can be scaled or adapted to future maritime standoffs or domestic political inflection points. U.S. partners in the region may face heightened challenges in attribution, internal cohesion, and strategic messaging under asymmetric pressure.

Potential Key Indicators

Expansion of prepositioned malware or persistent access from traditional civilian sectors into defense-adjacent logistics, emergency services, and contingency mobilization networks. Target shifts from general IT infrastructure to sectors and systems critical for national crisis response may indicate a transition from reconnaissance to coercive crisis positioning. These critical nodes include military logistics hubs, energy dispatch systems, or emergency response coordination centers.

Surge in cyber-enabled influence operations exploiting leadership transitions, emphasizing amplification of "economic pragmatism" or "strategic autonomy" narratives aligned with PRC interests. Indicators include disproportionate online boosting of politicians advocating trade de-escalation with the PRC, criticism of defense pacts, or narratives minimizing PRC security threats. These activities are especially concerning when amplified by AI-generated or inauthentic social media activity.

Cyber-enabled disruption, coercive ransomware, or pre-positioned wiper malware activity around critical minerals supply chains during resource realignment efforts. Early indicators include network reconnaissance of export control agencies, port authorities, or mining regulatory bodies, signaling preparation to impose friction, undermine enforcement, or retaliate against supply chain diversification.

Sustained Pressure on the U.S. Alliance Backbone

Beijing will expand cyber and influence operations to exploit shifting regional and alliance dynamics. Recent electoral shifts, internal E.U. divisions, and trade frictions have created contested spaces that Beijing actively seeks to influence.[308] [309] Cyber operations will likely prioritize intelligence collection on policymaking, technology decoupling, defense cooperation, and foreign investment strategies. These efforts will likely intensify where political fragmentation or economic pressures create tactical openings. Beijing's ultimate aim is to expand access, fracture policy alignment, and preserve strategic engagement opportunities in an increasingly contested global environment.

Beijing will sustain and deepen persistent cyber access to critical infrastructure and defense ecosystems across U.S. allies to support intelligence collection, contingency planning, and potential crisis leverage. Access to telecommunications, logistics, maritime, energy, and defense sectors provides Beijing with visibility into alliance strength and establishes operational options for disruption, surveillance, and deterrence.

Beijing's influence operations will intensify during periods of political turnover and strategic hedging among U.S. allies. These efforts are likely to focus on marginalizing adversarial figures, empowering accommodating or pragmatic actors, and reinforcing perceptions of the PRC as an indispensable economic and diplomatic partner. The broader objective is to sustain strategic access, fragment adversarial consensus, and erode the cohesion of U.S.-aligned security frameworks over time.

Beijing will escalate cyber operations targeting Five Eyes critical minerals sectors and economic policy bodies to counter allied efforts to reduce PRC leverage over strategic resources. Recent trends suggest a focus on collecting intelligence on supply chain diversification initiatives, influencing investment and trade policies, and disrupting emerging frameworks for critical minerals cooperation. Operations are likely to prioritize rare earths supply chains, regulatory agencies, and trade alliances that threaten the PRC's dominant position in global refining and export markets.[311] [312]

Potential Key Indicators

Sustained or expanded cyber access into decision-making ecosystems during alliance realignments. Indicators might include persistent intrusions into legal advisory teams, trade negotiation units, and legislative bodies, suggesting a strategic intent to monitor, anticipate, and subtly influence decision-making during periods of realignment or policy flux.

Increased reconnaissance and credential harvesting targeting critical minerals governance bodies. Focused activity against export control agencies, mining regulators, and logistics operators would indicate a priority to gain visibility into emerging supply chain strategies and to build options for future disruption or leverage if decoupling accelerates.

Steady growth of cyber-enabled influence operations exploiting leadership transitions in U.S. allies. Amplification of “economic pragmatism,” “strategic autonomy,” or anti-alignment narratives, particularly surrounding political figures advocating for reduced confrontation with the PRC, may indicate active efforts to shape elite discourse and weaken U.S.-aligned security cohesion.

Emerging persistence operations in logistics, emergency response, and mobilization networks of U.S. allies. Detection of targeted intrusions into systems coordinating military logistics, energy grid, or healthcare may indicate intent to create options for operational disruption during a future escalation.

Preemptive Influence and Embedded Access in the Developing World

PRC-linked influence operations are likely to expand in countries experiencing leadership transitions, economic strain, or diplomatic realignment. These conditions enable Beijing to shape elite and public opinion through asymmetric means. Activity across Africa, Latin America, and the Pacific shows a growing use of covert media assets, local proxies, and pseudo-local narratives to reinforce pro-PRC messaging and discredit foreign engagement. These campaigns appear designed to promote Beijing as a more stable, non-interfering partner while raising the reputational and political costs of deeper alignment with the U.S. and its allies.

Sustained cyber access to infrastructure in the developing world is likely to provide Beijing with operational leverage over competing diplomatic or defense engagements. PRC-linked threat actors have maintained persistent access to government and telecom networks across Africa and Latin America, including in countries with growing ties to the U.S. or Taiwan. This access enables real-time surveillance, influence over sensitive processes, and the potential to disrupt rival coordination during crises or negotiations. As more countries adopt PRC-built digital infrastructure, this leverage may extend to agenda-setting in multilateral forums or constraint of third-party basing and assistance.

PRC cyber campaigns are likely to intensify following early signals of alignment with PRC competitors. Beijing has historically escalated intrusion activity after shifts in diplomatic, defense, or economic posture, such as new U.S. compacts and Taipei engagements. These operations may aim to collect internal political data, undermine decision-makers, or preempt rival influence gains. As the PRC becomes more risk-tolerant and technically advanced, this behavior may evolve into a standing counter-alignment doctrine in cyberspace.

Cyber and information operations targeting Taiwan's diplomatic partners in the developing world are likely to focus on reputational erosion and exposure of informal engagement channels. These campaigns may exploit budgetary transparency, leaked communications, and targeted online influence operations to discredit Taipei-aligned governments or delegitimize Taiwan's international visibility. This behavior is likely to escalate around moments when alignment decisions are most vulnerable to external pressure, such as summits or compact renewals.

Future PRC gray-zone campaigns in the Pacific and Africa may blend cyber operations with overt diplomatic or economic pressure to reshape alignment outcomes. Recent campaigns, such as Operation Tainted Love and the Palau ransomware leak, have combined cyber intrusions with political signaling during U.S.-linked engagements. This indicates an evolving strategy to pair digital tools with traditional leverage points to create ambiguity, chill dissent, or sabotage rival momentum. These blended pressure tactics are likely to intensify in regions where PRC ambitions run up against growing external competition.

Potential Key Indicators

Sustained cyber access to foreign ministries, intelligence services, or elite policy nodes in the developing world aligned with PRC infrastructure projects or Taiwan policy. Detection of persistent access or renewed targeting of these institutions, particularly during infrastructure negotiations or policy inflection points, signals Beijing's interest in shaping sovereign decisions and preempting external influence.

Cyber-enabled disruption and leaks coinciding with diplomatic alignment shifts or security agreements. Ransomware or leak operations with weak financial incentives and strong signaling characteristics, especially timed to Taiwan or U.S. diplomatic engagement, may indicate an intent to impose cost or erode trust in non-PRC partnerships.

Intrusions into telecommunications and mobile network providers with ties to PRC-built infrastructure or vendor ecosystems. Compromise of regional telecoms and maintenance contractors may enable Beijing to preserve access, monitor strategic communications, and reinforce technical dependencies at scale.

Leak operations targeting political figures in fragile democracies. Campaigns that exfiltrate and leak sensitive information, particularly during multilateral negotiations or other charged political environments, may indicate cyber-enabled political warfare designed to influence outcomes without direct confrontation.

Emergence of AI-generated content in tandem with regional influence campaigns on contested topics such as Taiwan, the U.S., or allied infrastructure. The integration of generative AI into local-facing messaging, especially during moments of regional political friction, would signal operational maturation and scalable deployment of digital influence in strategically contested countries.

Recommendations

7

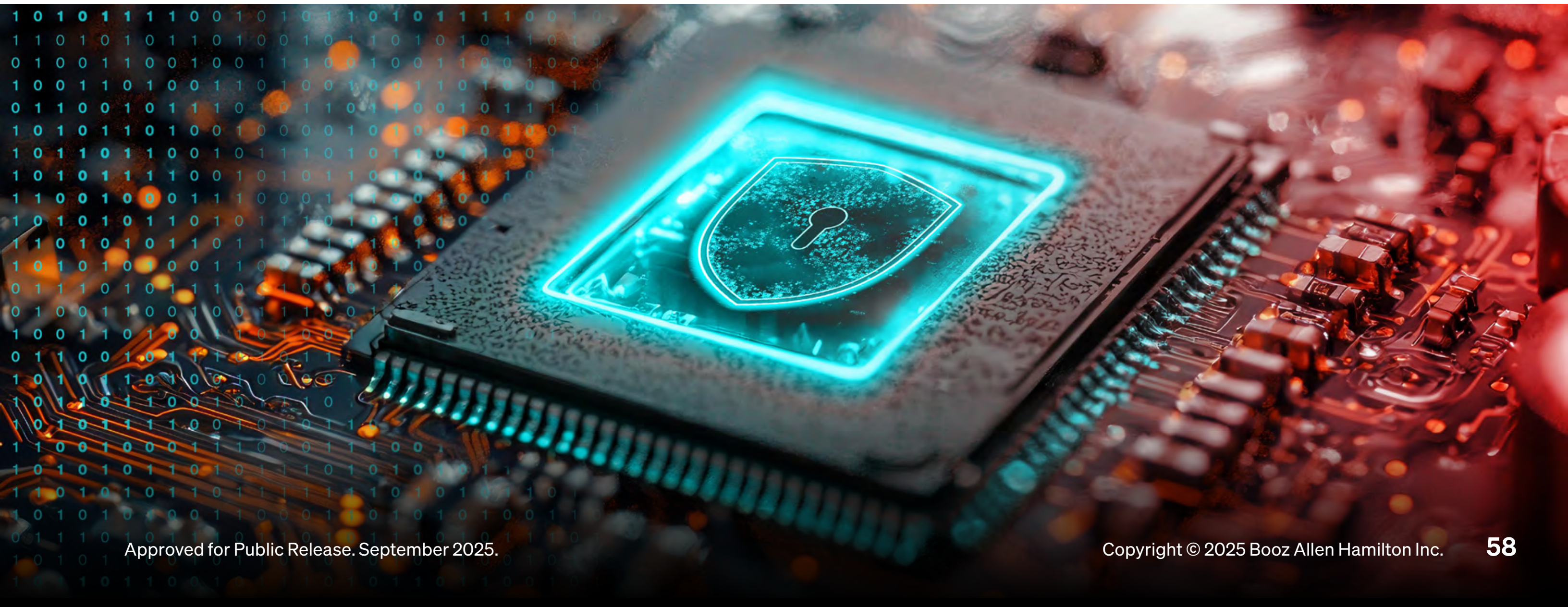
Recommendations

This section outlines a forward-leaning strategy to counter PRC cyber efforts to constrain the United States through coordinated technical, institutional, and geopolitical action. The recommendations span hardening edge infrastructure, disrupting access vectors, denying control over strategic systems, and reinforcing coalition resilience. At their core, these are operational countermeasures, meant to blunt Beijing's long-term leverage, expose covert positioning, and secure the terrain on which future crises may unfold.

Close the Trusted Back Door: Shut off Vendor Access as a Persistent Threat Channel

PRC threat actors exploit vendor relationships to maintain durable access inside hardened networks. Securing vendor access pathways closes high-risk gaps in U.S. defense and critical infrastructure systems, denying adversaries easy points of entry and persistent surveillance opportunities.

- **Apply zero trust (ZT) architecture principles to third-party access** by enforcing continuous authentication, least-privilege access, and behavioral monitoring, using the Department of Defense's phased ZT model to guide milestones and adoption metrics.
- **Segment and secure vendor-managed update mechanisms and support tooling** from broader production environments.
- **Deploy behavioral analytics on all vendor sessions**, flagging anomalies such as off-hours lateral movement or unusual credential usage.
- **Require continuous logging and auditing of all third-party access** to government, defense, and critical infrastructure systems.
- **Phase in just-in-time session brokering and centralized oversight for privileged vendor access**, starting with high-risk systems and using time-bound credentials, session logging, and restricted network paths as interim controls where full implementation is not yet feasible.
- **Conduct adversary emulation exercises** to test detection and response against vendor-side compromise scenarios.



Fortify the Edge: Treat Edge Infrastructure as Key Cyber Terrain

PRC threat actors are systematically exploiting firewalls, VPNs, and under-monitored communications infrastructure as persistent footholds. As targeting is projected to expand to space systems, industrial gateways, and telecom access points. Securing U.S. and allied edge infrastructure denies PRC actors persistent access to systems critical for military operations, economic stability, and crisis response.

- **Standardize and harden device configurations at scale,** including update pipelines, default disabling of remote administration, and removal of vendor-side access by contract.
- **Develop firmware telemetry and logging solutions for diverse edge assets** in ICS, space, and mobile battlefield environments where traditional endpoint detection and response (EDR) is not viable.
- **Integrate edge-layer devices into core threat detection,** including passive monitoring of satellite terminals, carrier-grade network address translation (GNAT) equipment, and cellular gateways.
- **Apply ZT principles across edge environments** by verifying device integrity, embedding behavior-based monitoring, and enabling policy enforcement in low-visibility or resource-constrained edge assets to detect and contain adversary footholds before lateral spread.

Build and Buy Secure: Reorient Software and Hardware Procurement and Production Around Adversarial Control Risk

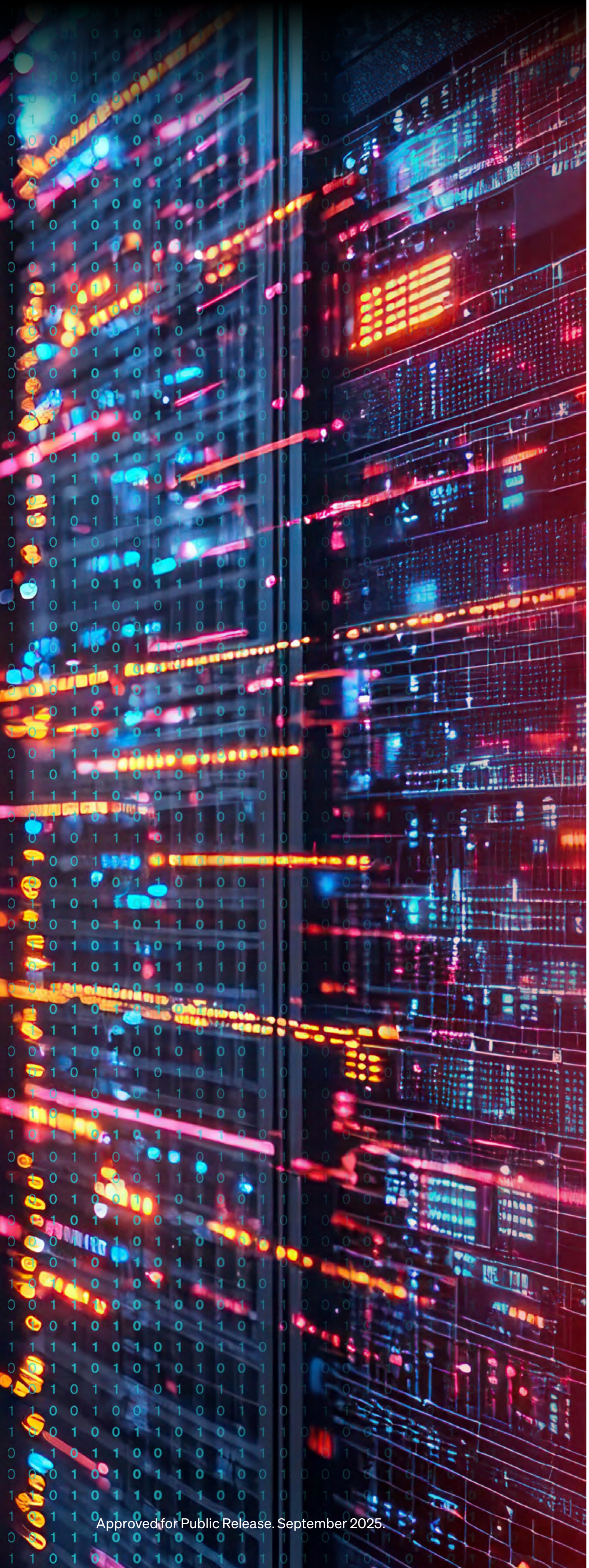
Protecting U.S. systems requires a pragmatic procurement approach that integrates national security risk without stifling innovation. In addition to technical assessments, procurement processes should account for systemic risk stemming from adversarial control, particularly when devices, platforms, and their specific components originate from or are influenced by jurisdictions with state-aligned access obligations. Mitigating adversarial hardware and firmware risk protects U.S. defense systems, critical infrastructure, and communications networks from exploitation and coercion.

- **Strengthen federal procurement standards** to incentivize secure-by-design networking technologies, favoring vendors that demonstrate transparency, verifiable supply chains, and insulation from adversarial influence, while preserving innovation and competition through clear, risk-based criteria.
- **Establish a federal hardware and firmware risk register to identify technologies exposed to PRC control risk,** enabling agencies to prioritize and phase out vulnerable edge and remote management systems.
- **Establish a standardized framework for assessing adversarial control risks** in procurement, factoring in vendor ownership, update authority, and jurisdictional exposure, with priority on high-impact systems and alignment to national security objectives.
- **Factor structural state-aligned risks,** such as PRC disclosure laws and covert update mechanisms, into procurement decisions and security compliance reviews, emphasizing transparency and operational control over hard exclusion lists.

Burn the Botnet and Relay Layer: Target and Disrupt Infrastructure Provisioning Ecosystems

The PRC's use of contractor-supported botnets, anonymization relays, and hijacked infrastructure creates persistent operational reach and degrades attribution. Disrupting PRC-controlled infrastructure networks weakens adversary operational reach, complicates long-term access to U.S. and allied systems, and raises the cost of persistent espionage and influence operations targeting American interests.

- **Map infrastructure abuse patterns,** focusing on relay networks, virtual private server (VPS) abuse, and regional ISP hijacking.
- **Develop disruption mechanisms** targeting provisioning actors, not just front-line operators.
- **Prioritize takedown and blocking actions** against PRC-linked firms supplying infrastructure for espionage or influence operations.
- **Focus infrastructure disruption efforts on strategic environments,** including industrial control systems / supervisory control and data acquisition (ICS/SCADA) systems, telecom backbones, and satellite networks.
- **Sustain dedicated threat hunting teams** to track botnet reuse, shared exploits, and reseller networks enabling PRC campaigns.
- **Target the ecosystem of infrastructure brokers and botnet operators** supporting PRC-linked activity, using combined legal, regulatory, and technical action to degrade operational reach.



Out-Automate the Adversary: Overmatch and Degrade PRC AI-Powered Automation

PRC cyber and influence operators are leveraging AI to automate reconnaissance, generate tailored phishing content, and scale influence operations. U.S. efforts must both outpace these capabilities and actively degrade their effectiveness. This requires fielding AI systems that accelerate analyst workflows, improve detection of malign activity, and reduce attacker dwell time. Concurrently, the U.S. must also develop counter-AI techniques to disrupt PRC model performance and reliability. The focus should be on practical, testable capabilities that integrate into existing tooling, support real-world disruption, and hold up under adversarial pressure.

- **Develop and deploy AI models for incident triage and signal extraction**, capable of rapidly correlating alerts and prioritizing potential intrusions based on behavioral patterns.
- **Field content analysis and influence detection tools** with a focus on cross-platform tracking of known influence vectors, amplification patterns, and PRC-linked persona reuse targeting U.S. partners.
- **Integrate AI into cyber red-teaming workflows,** including automated open-source intelligence (OSINT) collection and use of generative models to produce convincing decoys and lures.
- **Apply strict governance, auditability, and supply chain verification for all AI systems used in defense operations,** ensuring they meet reliability thresholds under adversarial pressure and are viable for classified or sensitive environments.
- **Develop methods to detect, mislead, or confuse PRC-deployed AI systems**, including influence automation, targeting workflows, and malware generation tools.
- **Develop and field counter-AI techniques—such as model inversion, evasion, and poisoning**—to undermine PRC AI model performance supporting reconnaissance and influence operations.

Fight the Attribution Fight: Address Attribution as a Contested and Strategic Space

The PRC is blurring responsibility and contesting attribution to erode accountability. Sustaining credible, high-confidence attribution at speed requires strengthening the public-private ecosystem, not just internal IC processes.

- **Enhance analytic collaboration with the private sector,** creating declassification pathways and legal protections to support high-confidence public attribution against PRC-linked actors.
- **Strengthen public attribution efforts** by coordinating messaging that reinforces high-confidence, evidence-based findings across government and trusted private sector sources.
- **Synchronize public attribution messaging** across intelligence, law enforcement, diplomatic, and private sector partners to preempt PRC denials and reinforce coherent, credible disclosures.

Break the Influence Chain: Map, Expose, and Dismantle PRC Covert Online Influence Networks

The PRC is running hostile covert online influence campaigns to manipulate U.S. allies and fracture key relationships. This is information warfare, mobilizing front groups, criminals, commercial businesses, and intelligence proxies to shape decisions, sway opinion, and suppress dissent. The U.S. should go beyond fact-checking and civil society capacity-building to actively disrupt the infrastructure, networks, and operators that enable and conduct the PRC's covert online information campaigns. Pushing back at the source will constrain Beijing's reach and restore U.S. initiative.

- **Develop cross-platform content tracing tools** to detect narrative amplification and migration between fringe and mainstream channels, enabling earlier identification of coordinated influence campaigns.
- **Integrate real-time detection of synthetic media** e.g., deepfakes) into influence monitoring systems to flag inauthentic personas and forged content before they gain traction.
- **Map and disrupt influence propagation pathways** by integrating real-time narrative tracking into interagency watch centers and allied early warning systems.
- **Disrupt provisioning networks** for sockpuppet and hijacked social media accounts that enable large-scale covert messaging operations.
- **Conduct forward cyber operations** to dismantle key elements of foreign influence infrastructure, including troll farms, fake news hubs, and botnets.
- **Generate shareable intelligence on PRC proxy networks** targeting allies and partners—including front companies, financial conduits, and covert infrastructure—to support collaborative exposure, legal action, and sanctions.
- **Conduct information operations wargames with U.S., allied, and partner agencies** to train strategic-level decision-making under narrative attack stresses—testing coordination, escalation triggers, and policy responses.

Forward-Posture with Partners: Strengthen U.S. Cyber Posture Across the PRC's Eastern Strategic Periphery

The PRC is using cyber and information operations across East Asia to weaken allied crisis response, fracture pro-U.S. political alignments, and extract critical technologies for strategic gain. These efforts could delay regional mobilization, undermine U.S. influence, and entrench Beijing's advantage in future contingencies. Proactive U.S. action can preserve escalation dominance, protect access to critical systems, and strengthen front-line allies against PRC coercion.

- **Harden critical communications, logistics, and mobilization nodes** in Taiwan, Japan, and the Philippines through cyber resilience partnerships and bilateral contingency planning.
- **Expand intelligence support and rapid influence forensics** to expose and counter PRC political warfare campaigns targeting pro-U.S. leaders.
- **Secure advanced technology pipelines** by integrating Taiwan and Japan's critical sectors into U.S. defense-industrial cybersecurity frameworks and bilateral threat intelligence exchanges.
- **Disrupt persistent PRC cyber access** to defense-relevant infrastructure by funding threat hunting partnerships and pre-crisis exposure campaigns to deny Beijing escalation leverage.
- **Preemptively position U.S. and allied defensive cyber teams with regional partners** to enable early threat detection, live-fire training, and rapid response planning, denying PRC actors uncontested access during periods of elevated tension and reinforcing coalition readiness before crises emerge.

Draw Allies Closer: Defend Alliance Resilience Against PRC Cyber and Influence Operations

The PRC is exploiting political fractures, economic vulnerabilities, and policy realignments across Europe and the Five Eyes to weaken U.S.-aligned coalitions and entrench its strategic access. Cyber and influence operations target decision-making ecosystems, critical infrastructure, and political leadership to delay coordinated action and normalize Beijing's presence. Without sustained U.S. action, alliance cohesion may erode under pressure, slowing crisis response and ceding ground to PRC influence.

- **Expand cyber defense cooperation with European and Five Eyes partners**, prioritizing the protection of decision-making ecosystems, mobilization nodes, and critical infrastructure essential to defense and crisis response operations.
- **Strengthen attribution and influence forensics partnerships**, embedding pre-crisis attribution playbooks and enabling allies to rapidly detect, attribute, and expose PRC cyber and influence operations.
- **Defend critical mineral supply chains** by hardening partner networks, protecting regulatory and export control agencies, and exposing PRC cyber campaigns targeting diversification efforts.
- **Fund forward-deployed cyber resilience teams**, operating by host-nation invitation, to assist allies in detecting, disrupting, and evicting persistent PRC access from logistics, telecommunications, energy, and mobilization sectors.
- **Prioritize technical and intelligence support** for partners whose cyber resilience efforts directly reinforce collective alignment and strategic cohesion against PRC pressure.

Deny Digital Entrenchment: Dislodge PRC Leverage in the Developing World

The PRC is embedding surveillance footholds and technical dependencies across Africa, Latin America, and the Pacific Islands that risks restricting U.S. maneuverability and obstructing access. Proactive cyber operations in these regions help deny Beijing uncontested terrain. Deploying capability-forward partnerships enables the U.S. to secure critical infrastructure, lock out adversary access, and shape conditions before geopolitical pressure points harden into crises.

- **Fund targeted technical operations** to secure telecoms, cloud services, and software platforms deployed by PRC-linked firms.
- **Embed cyber liaison teams** with at-risk governments to harden networks, counter PRC intrusions, and secure environments critical to U.S. regional access.
- **Enable trusted partners to conduct their own attribution and exposure of PRC operations**, reducing overreliance on U.S. disclosures, accelerating response timelines, and increasing reputational costs for Beijing.
- **Organize regular red team and blue team exercises** with government and infrastructure operators managing PRC-origin platforms, building readiness in locations vital to U.S. regional posture.

Conclusion

8

The scale, stealth, speed, and deniability of PRC-linked cyber operations demand a sharper understanding of what is changing and why it matters. While scores of incidents are well documented, their strategic coherence is often obscured by technical diversity, geographic spread, and the relentless day-to-day demands of network defense. This report shows how Beijing has honed key operational methods through national-level efforts, tailored them to local conditions, and aligned them to global objectives to quietly shift the terms of strategic competition in its favor.

These are not isolated incidents to be remediated, documented, and filed away. They are expressions of a coherent national effort, supported by tailored legal, technical, and industrial structures that enable scale, stealth, and persistence. Whether exploiting network edges, trusted vendors, or AI-accelerated reconnaissance, PRC actors are methodically shaping adversary operating environments to degrade responsiveness, fracture alignment, and raise the cost of pushback. This is not simply intrusion. It is erosion—of initiative, resilience, and freedom of action.

A national response must match the scale and structure of the threat. That means modernizing cyber defenses to prioritize edge access and vendor risk, contesting attribution with speed and credibility, and aligning regional strategies to counter PRC leverage across infrastructure, diplomacy, and influence. Above all, it requires a shift in posture—from reacting to adversary campaigns to shaping the operating environment ourselves. Strategic initiative is not lost all at once. It is conceded in increments. This report provides a map to stop that slide. The window for action is narrowing. The U.S. must act now to dislodge embedded threats and reassert the strategic initiative.

Citations

9

Citations

1 CHINA MFA Spokesperson 中国外交部发言人 , “Never Kneel Down!,” Instagram, April 29, 2025, July 14, 2025, https: //www. instagram. com/mfa_china/reel/DJGEB2-R4AD/.

2 Military and Security Developments Involving the People’s Republic of China 2024, U.S. Department of Defense, n.d., accessed May 5, 2025, https: //media. defense. gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024. PDF.

3 Tim Starks, "‘Whatever we did was not enough’: How Salt Typhoon slipped through the government’s blind spots," Cyberscoop, May 20, 2025, accessed May 27, 2025, https: //cyberscoop. com/salt-typhoon-us-government-response/.

4 Julian Borger, “US ambassador to Beijing targeted in Chinese cyber-attack – report,” The Guardian, July 20, 2023, accessed May 27, 2025, https: //www. theguardian. com/us-news/2023/jul/20/ambassador-to-beijing-among-us-officials-hit-by-chinese-hackers.

5 “How to Outpace Cyber Threats to Critical Infrastructure” Booz Allen, 2023, accessed May 27, 2025, https: //www. boozallen. com/content/dam/home/docs/ns-viewpoints/national-cyber-viewpoints-how-to-outpace-cyber-threats. pdf.

6 Yimou Lee, "Taiwan says China behind cyberattacks on government agencies, emails," Reuters, August 19, 2020, accessed May 5, 2025, https: //www. reuters. com/article/us-taiwan-cyber-china/taiwan-says-china-behind-cyberattacks-on-government-agencies-emails-idUSKCN25F0JK/.

7 Yimou Lee, "Taiwan says China behind cyberattacks on government agencies, emails," Reuters, August 19, 2020, accessed May 5, 2025, https: //www. reuters. com/article/us-taiwan-cyber-china/taiwan-says-china-behind-cyberattacks-on-government-agencies-emails-idUSKCN25F0JK/.

8 Yimou Lee, "Taiwan says China behind cyberattacks on government agencies, emails," Reuters, August 19, 2020, accessed May 5, 2025, https: //www. reuters. com/article/us-taiwan-cyber-china/taiwan-says-china-behind-cyberattacks-on-government-agencies-emails-idUSKCN25F0JK/.

9 "Silk Typhoon targeting IT supply chain," Microsoft, March 5, 2025, accessed May 5, 2025, https: //www. microsoft. com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/.

10 "Patch Now: Check Point Research Explains Shadow Pad, NailaoLocker, and its Protection," Check Point, February 21, 2025, accessed May 5, 2025, https: //www. scrible. com/view/source R2IO1COL20LQG2MG3443K8O48P4CM20E: 1424161239/.

11 Aleksandar Milenkoski and Luigi Martire, “Operation Digital Eye | Chinese APT Compromises Critical Digital Infrastructure via Visual Studio Code Tunnels,” SentinelOne, December 10, 2024, accessed May 5, 2025, https: //www. sentinelone. com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/.

12 Tom Hegel, Aleksandar Milenkoski & Jim Walter, "Top Tier Target | What It Takes to Defend a Cybersecurity Company from Today’s Adversaries," SentinelOne, April 28, 2025, accessed May 5, 2025, https: //www. sentinelone. com/labs/top-tier-target-what-it-takes-to-defend-a-cybersecurity-company-from-todays-adversaries/.

13 Lucian Constantin, "40 Enterprise Computers Infected with Second-Stage CCleaner Malware," Security Boulevard, September 26, 2017, accessed May 5, 2025, https: //securityboulevard. com/2017/09/40-enterprise-computers-infected-second-stage-ccleaner-malware/.

14 Swati Khandelwal, "Here's the List of ~600 MAC Addresses Targeted in Recent ASUS Hack," The Hacker News, March 29, 2019, https: //thehackernews. com/2019/03/asus-hack-mac-addresses. html.

15 "Operation ShadowHammer: new supply chain attack threatens hundreds of thousands of users worldwide," Kaspersky, March 25, 2019, accessed May 5, 2025, https: //www. kaspersky. com/about/press-releases/operation-shadowhammer-new-supply-chain-attack.

16 Christopher Glyer, Dan Perez, Sarah Jones, Steve Miller, "This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits," Mandiant, March 25, 2020, accessed May 5, 2025, https: //cloud. google. com/blog/topics/threat-intelligence/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.

17 Christopher Glyer, Dan Perez, Sarah Jones, Steve Miller, "This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits," Mandiant, March 25, 2020, accessed May 5, 2025, https: //cloud. google.om/blog/topics/threat-intelligence/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.

18 “Additional Activities of the Tick Group That Attacks with a Modified Q-Dir and Their Ties with Operation Triple Tiang,” Ahn Lab, April 10, 2023, accessed May 5, 2025, https: //asec. ahnlab. com/en/51340/.

19 “Threat Trend Report on Operation Triple Tiang,” AhnLab Security Emergency Response Center, March 31, 2022, accessed May 5, 2025, https: //web. archive. org/web/20230316010626/https: //download. ahnlab. com/global/brochure/03.%20ATIP_Threat%20Trend%20Report%20on%20Operation%20Triple%20Tiang. pdf.

20 "Carderbee: APT Group use Legit Software in Supply Chain Attack Targeting Orgs in Hong Kong" Symantec, last modified August 22, 2023, accessed May 5, 2025, https: //www. security. com/threat-intelligence/carderbee-software-supply-chain-certificate-abuse.

[21] Facundo Muñoz, "Evasive Panda APT group delivers malware via updates for popular Chinese software," ESET, April 26, 2023, accessed May 5, 2025, https: // www. welivesecurity. com/2023/04/26/ evasive-panda-apt-group-malware-updates-popular-chinese-software/.

[22] Ankur Saini, Paul Rascagneres, Steven Adair, Tom Lancaster, "StormBamboo Compromises ISP to Abuse Insecure Software Update Mechanisms," Volexity, August 2, 2024, accessed May 5, 2025, https: //www. volexity. com/blog/2024/08/02/ stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/.

[23] Facundo Muñoz, “PlushDaemon compromises supply chain of Korean VPN service,” ESET, January 22, 2025, accessed May 5, 2025, https: //www. welivesecurity. com/en/eset-research/ plushdaemon-compromises-supply-chain-korean-vpn-service/.

[24] Facundo Muñoz, “TheWizards APT group uses SLAAC spoofing to perform adversary-in-the-middle attacks,” ESET, April 30, 2025, accessed May 5, 2025, https: // www. welivesecurity. com/en/eset-research/ thewizards-apt-group-slaac-spoofing-adversary-in-the-middle-attacks/.

[25] Facundo Muñoz, “TheWizards APT group uses SLAAC spoofing to perform adversary-in-the-middle attacks,” ESET, April 30, 2025, accessed May 5, 2025, https: // www. welivesecurity. com/en/eset-research/ thewizards-apt-group-slaac-spoofing-adversary-in-the-middle-attacks/.

[26] "Adobe To 'Sandbox' PDF Files," Dark Reading, July 20, 2010, accessed May 6, 2025, https: //www. darkreading. com/cyber-risk/adobe-to-sandbox-pdf-files.

[27] Gilad David Maayan, "A Brief History of EDR Security," DZone, April 7, 2020, accessed May 6, 2024, https: // dzone. com/articles/a-brief-history-of-edr-security/.

[28] John Lambert, “Early Security Stories — ASLR,” Medium, December 28, 2019, accessed May 6, 2025, https: //medium. com/@ johnlatwc/ early-security-stories-aslr-4c6bafe0dda1.

[29] Ian Shine, "Where remote jobs are growing fastest - 4 charts show the locations and sectors," World Economic Forum, April 3, 2023, accessed May 6, 2025, https: //www. weforum. org/stories/2023/04/ remote-jobs-growing-fastest-locations-sectors/.

[30] "Charting China’s Climb as a Leading Global Cyber Power," Recorded Future, November 7, 2023, accessed May 6, 2025, https: //go. recordedfuture. com/hubfs/ reports/cta-2023-1107. pdf.

[31] "We’re All in this Together: A Year in Review of Zero-Days Exploited In-the-Wild in 2023," Google, March 2024, accessed May 6, 2025, https: //storage. googleapis. com/gweb-uniblog-publish-prod/ documents/Year_in_Review_of_ZeroDays. pdf.

[32] Casey Charrier et al., “Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis,” Google Threat Intelligence, April 29, 2025, accessed July 8, 2025, https: //cloud. google. com/blog/topics/ threat-intelligence/2024-zero-day-trends.

[33] Lucian Costantin, "Top 7 zero-day exploitation trends of 2024," CSO, December 23, 2024, May 6, 2025, https: // www. csoonline. com/article/3629815/top-7-zero-day-exploitation-trends-of-2024. html.

[34] “Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets,” Recorded Future, September 22, 2022, accessed May 6, 2025, https: //go. recordedfuture. com/hubfs/reports/ cta-2022-0922.pdf, pp. 3.

[35] “Aanhoudende statelijke cyberspionagecampagne via kwetsbare edge devices [Ongoing state-sponsored cyber-espionage campaign targeting vulnerable edge devices.],” National Cybersecurity Center, June 10, 2024, accessed May 6, 2025, https: //www. ncsc. nl/ actueel/nieuws/2024/juni/10/ aanhoudende-statelijke-cyberspionagecampagne-via-kwetsbare-edge-devices.

[36] “Chinese Fortigate hack was much bigger: Dutch spy service says,” DutchNews, June 10, 2024, accessed May 6, 2025, https: //www. dutchnews. nl/2024/06/ chinese-fortigate-hack-was-much-bigger-dutch-spy-service-says.

[37] Casey Charrier, James Sadowski, Clement Lecigne, Vlad Stolyarov, "Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis," Google, April 29, 2025, accessed May 6, 2025, https: //cloud. google. com/ blog/topics/threat-intelligence/2024-zero-day-trends.

[38] Dakota Cary and Kristin Del Rosso, "Sleight of hand: How China weaponizes software vulnerabilities," Atlantic Council, September 6, 2023, accessed May 6, 2025, https: //www. atlanticcouncil. org/in-depth-research-reports/report/ sleight-of-hand-how-china-weaponizes-software-vulnerability/.

[39] Ross McKerchar and Andrew Brandt, "Pacific Rim timeline: Information for defenders from a braid of interlocking attack campaigns - CVE-2022-1040 (‘Personal Panda’)," Sophos, October 31, 2024, accessed May 6, 2025, https: //news. sophos. com/ en-us/2024/10/31/ pacific-rim-timeline/#_Personal_Panda.

[40] Michael Raggi, "IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders," Google, May 22, 2024, accessed May 6, 2025, https: //cloud. google. com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks/.

[41] Federal Bureau of Investigation et al., "People’s Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations," n.a., September 18, 2024, https: //media. defense. gov/2024/ Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET. PDF.

42 Binayak Dasgupta, "Chinese hackers targeted 7 Indian power hubs, govt says ops failed," Hindustan Times, April 8, 2022, accessed May 6, 2025, https: //www. hindustantimes. com/india-news/chinese-hackers-targeted-7-indian-power-hubs-govt-says-ops-failed-101649356540330. html.

43 “People’s Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action,” CISA, July 8, 2024, accessed May 16, 2025, https: //www. cisa. gov/news-events/cybersecurity-advisories/aa24-190a.

44 “Weaver Ant, the Web Shell Whisperer: Tracking a Live China-nexus Operation,” Sygna, March 24, 2025, accessed May 16, 2025, https: //www. sygnia. co/threat-reports-and-advisories/weaver-ant-tracking-a-china-nexus-cyber-espionage-operation/.

45 "Court-Authorized Operation Disrupts Worldwide Botnet Used by People’s Republic of China State-Sponsored Hackers," U.S. Department of Justice, September 18, 2024, accessed May 6, 2025, https: //www. justice. gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state.

46 Federal Bureau of Investigation et al., "People’s Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations," n.a., September 18, 2024, https: //media. defense. gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET. PDF.

47 "From Coercion to Invasion: The Theory and Execution of China’s Cyber Activity in Cross-Strait Relations," Recorded Future, November 23, 2022, accessed May 6, 2025, https:/ /www. recordedfuture. com/research/from-coercion-to-invasion-the-theory-and-execution-of-china-cyber-activity.

48 “Supply Chain Analysis: From Quartermaster to SunShop,” FireEye, 2014, archived October 7, 2022, https: //web. archive. org/web/20221007195611/https: //www. mandiant. com/sites/default/files/2021-09/rpt-malware-supply-chain. pdf.

49 Justin Sherman and Robert Morgus, “Not Every Huawei Flaw Is a Backdoor,” New America, May 9, 2019, accessed June 26, 2025, https: //www. newamerica. org/weekly/not-every-huawei-flaw-backdoor/.

50 Heather Somerville , Dustin Volz and Aruna Viswanatha, "U.S. Weighs Ban on Chinese-Made Router in Millions of American Homes," Wall Street Journal, December 18, 2024, archived December 20, 2024, https: //archive. is/SH8NK.

51 K. Christopher Powell, "U.S. Defense Dept Purchased Chinese IT Equipment with Known Vulnerabilities for Use at Sensitive Base." The National Pulse, February 24, 2023, accessed May 6, 2025, https: //thenationalpulse. com/archive-post/u-s-defense-dept-purchased-chinese-it-equipment-with-known-vulnerabilities-for-use-at-sensitive-base/.

52 Jack Corrigan et al., “Banned in D.C.: Examining Government Approaches to Foreign Technology Threats,” CSET, October 2022, accessed May 16, 2025, https: //cset. georgetown. edu/wp-content/uploads/CSET-Banned-in-D.C.-1. pdf, p. 23.

53 Bernard Meyer, “Walmart-exclusive router and others sold on Amazon & eBay contain hidden backdoors to control devices,” Cybernews, November 2, 2022, accessed May 21, 2025, https: //cybernews. com/security/walmart-exclttive-routers-others-made-in-china-contain-backdoors-to-control-devices/.

54 Sarah Mcfarlane, “Rogue communication devices found in Chinese solar power inverters,” Reuters, May 14, 2025, accessed May 21, 2025, https:/www. reuters. com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/.

55 Aruna Viswanatha et al., “Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools,” Wall Street Journal, last updated March 5, 2023, archived March 21, 2024, https: //archive. is/U7elt.

56 “Investigation by Select Committee on the CCP, House Homeland Finds Potential Threats to U.S. Port Infrastructure Security from China,” The Select Committee on the CCP, September 12, 2024, https: //selectcommitteeontheccp. house. gov/media/press-releases/investigation-select-committee-ccp-house-homeland-finds-potential-threats-us.

57 Jordan Robertson, "Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role," Bloomberg, September 2, 2021, accessed May 6, 2025, https: //www. bloomberg. com/news/features/2021-09-02/juniper-mystery-attacks-traced-to-pentagon-role-and-chinese-hackers.

58 Dan Perez, Sarah Jones, Greg Wood, Stephen Eckels, "Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day," Google, April 21, 2021, accessed May 6, 2025, https: //cloud. google. com/blog/topics/threat-intelligence/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day/.

59 David Morgan, “FBI probes counterfeit China computer parts,” Reuters, May 9, 2008, accessed May 6, 2025, https: //www. reuters. com/article/technologyNews/idUSN0952813820080510/.

60 “Counterfeit Chinese Technology: Gateway for Hackers?,” ABC News, last modified February 23, 2009, accessed May 6, 2025, https: //abcnews. go. com/TheLaw/FedCrimes/story?id=4825112&page=1.

[61] Rual Roldan et al., “FBI Criminal Investigation: Cisco Routers,” Federal Bureau of Investigation, January 11, 2008, archived January 5, 2012, https: //web. archive. org/web/20120505004423/https: //www. andovercg. com/datasheets/0-FBI-Counterfeit-Cisco-Briefing-2008-01-11-a. pps.

[62] "Leader of Massive Scheme to Traffic in Fraudulent and Counterfeit Cisco Networking Equipment Sentenced to Prison," U.S. Department of Justice, May 2, 2024, accessed May 6, 2025, https: //www. justice. gov/archives/opa/pr/leader-massive-scheme-traffic-fraudulent-and-counterfeit-cisco-networking-equipment.

[63] “新时代的中国国防 [China’s National Defense in the New Era],” State Council Information Office, July 2019, accessed May 6, 2025, http: //www. gov. cn/zhengce/2019-07/24/content_5414325. htm.

[64] Nathan Beauchamp-Mustafaga, "Chinese Next-Generation Psychological Warfare," RAND, June 1, 2023, accessed May 6, 2025, https: //www. rand. org/pubs/research_reports/RRA853-1.html, p. 112-115.

[65] Edward Wong et al., "Chinese Spy Agency Rising to Challenge the C.I.A.," New York Times, December 27, 2023, accessed May 6, 2025, https: //www. nytimes. com/2023/12/27/us/politics/china-cia-spy-mss. html.

[66] “Disrupting malicious uses of our models: an update,” OpenAI, February 2025, accessed May 6, 2025, https: //cdn. openai. com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf, p. 7.

[67] Dina Temple-Raston, “China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying,” NPR, August 21, 2021, accessed May 6, 2025, https: //www. npr. org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.

[68] “Influence and cyber operations: an update,” OpenAI, October 2024, accessed May 6, 2025, https: //cdn. openai. com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024. pdf.

[69] “Staying ahead of threat actors in the age of AI,” Microsoft, February 14, 2024, accessed May 6, 2025, https: //www. microsoft. com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/.

[70] Nate Beach-Westmoreland, “Sharpening the Spear: China’s Information Warfare Lessons from Ukraine,” 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), May 30, 2023, accessed May 6, 2025, https: //ieeexplore. ieee. org/document/10181559.

[71] Jared Cohen and George Lee, "The generative world order: AI, geopolitics, and power," Goldman Sachs, December 14, 2023, accessed May 6, 2025, https: //www. goldmansachs. com/insights/articles/the-generative-world-order-ai-geopolitics-and-power.

[72] Koichiro Takagi, "Koichiro Takagi," War on the Rocks, April 13, 2022, accessed May 6, 2025, https: //warontherocks. com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare/.

[73] Iida Masafumi, “China’s Chilling Cognitive Warfare Plans,” The Diplomat, May 5, 2024, accessed May 6, 2025, https: //thediplomat. com/2024/05/chinas-chilling-cognitive-warfare-plans/.

[74] Nathan Beauchamp-Mustafaga, "Chinese Next-Generation Psychological Warfare," RAND, June 1, 2023, accessed May 6, 2025, https: //www. rand. org/pubs/research_reports/RRA853-1. html, p. 112-115.

[75] “Disrupting malicious uses of our models: an update,” OpenAI, February 2025, accessed May 6, 2025, https: //cdn. openai. com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update. pdf, p. 5.

[76] Iida Masafumi, “China’s Chilling Cognitive Warfare Plans,” The Diplomat, May 5, 2024, accessed May 6, 2025, https: //thediplomat. com/2024/05/chinas-chilling-cognitive-warfare-plans/.

[77] Nathan Beauchamp-Mustafaga, “Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations,” RAND, February 1, 2024, accessed May 6, 2025, https: //www. rand. org/content/dam/rand/pubs/testimonies/CTA3100/CTA3191-1/RAND_CTA3191-1. pdf.

[78] "Adversarial Misuse of Generative AI," Google Cloud, January 29, 2025, accessed May 6, 2025, https://cloud. google. com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai.

[79] "Green Cicada Network: Emerging X (Twitter) inauthentic account network powered by generative AI," CyberCX, August 13, 2024, accessed May 6, 2025, https: //connect. cybercx. com. au/Intelligence-Update-CCX-IU-2024-004.

[80] Thomas Shrimpton, “Chinese Military Seeking To Use AI Disinformation Database for Cognitive Defense,” OEWatch, 2003, accessed May 6, 2025, https: //community. apan. org/wg/tradoc-g2/fmso/m/oe-watch-past-issues/440811/download, p. 8-9.

[81] “Deepfake It Till You Make It: Pro-Chinese Actors Promote AI-Generated Video Footage of Fictitious People in Online Influence Operation,” Graphika, February 2023, accessed May 6, 2025, https: //public-assets. graphika. com/reports/graphika-report-deepfake-it-till-you-make-it. pdf.

[82] Adam Satariano and Paul Mozur, "The People Onscreen Are Fake. The Disinformation Is Real.," The New York Times, February 7, 2023, archived December 27, 2024, https: //archive. is/iBg9G.

83 “国家安全部党委书记、部长陈一新：加强数字时代的国家安全治理 [Chen Yixin, Party Secretary and Minister of the Ministry of State Security: Strengthen National Security Governance in the Digital Age],” Chinese Community Party News Network, September 26, 2023, archived November 23, 2023, https: //archive. ph/ IDTQ7.

84 Prashant Loyalka, “Computer science skills across China, India, Russia, and the United States,” PNAS, March 18, 2019, accessed May 6, 2025, https: //www. pnas. org/doi/10. 1073/pnas. 1814646116.

85 “Security Brief: Artificial Sweetener: SugarGh0st RAT Used to Target American Artificial Intelligence Experts,” Proofpoint, May 16, 2024, accessed May 6, 2025, https: //www. proofpoint. com/us/blog/threat-insight/ security-brief-artificial-sweetener-sugargh0st-rat-used-target-american.

86 “Influence and cyber operations: an update,” OpenAI, October 2024, accessed May 6, 2025, https: //cdn. openai. com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024. pdf.

87 Arjun Kharpal, "ASML blocked from shipping some of its critical chipmaking tools to China," CNBC, last modified January 2, 2024, accessed May 6, 2025, https: //www. cnbc. com/2024/01/02/asml-blocked-from-exporting-some-critical-chipmaking-tools-to-china. html.

88 John Lee & Jan-Peter Kleinhans, "Mapping China’s semiconductor ecosystem in global context" Stiftung Neue Verantwortung, June 2021, accessed May 21, 2025, https: //merics. org/sites/default/files/2021-06/ China%E2%80%99s%20Semiconductor%20 Ecosystem_0. pdf.

89 “How to Succeed at Annexation Without Really Fighting,” Booz Allen Hamilton, 2024, accessed May 6, 2025, https: //www. boozallen. com/content/dam/ home/pdf/cyber/national-cyber-how-to-succeed-at-annexation-without-fighting. pdf, p 28-29.

90 Yimou Lee and Sarah Wu, "'Tip of the iceberg': Taiwan's spy catchers hunt Chinese poachers of chip talent," Reuters, April 8, 2024, accessed May 6, 2025, https: // www. reuters. com/world/asia-pacific/ tip-iceberg-taiwans-spy-catchers-hunt-chinese-poachers-chip-talent-2022-04-08/.

91 Anton Shilov, “China's chip imports boom as the country stockpiles before anticipated new sanctions, struggles to become self-sufficient,” Tom’s Hardware, August 8, 2024, accessed May 6, 2025, https: //www. tomshardware. com/tech-industry/ chinas-chip-imports-boom-as-the-country-stockpiles-before-anticipated-new-sanctions-struggles-to-become-self-sufficient.

92 Dan Robinson, “The chips are down in China as imports see largest ever drop,” The Register, January 16, 2024, accessed May 6, 2025, https: //www. theregister. com/2024/01/16/china_chip_imports_fall/.

93 Lu Chuanying and Zhang Luyao, “A Chinese Perspective on Public Cyber Attribution,” China Quarterly of International Strategic Studies, 2022, accessed May 14, 2025, 2025, https: //www. worldscientific. com/doi/pdf/ 10. 1142/ S2377740022500026?srsltid=AfmBOoois COcX0qZsQORJoeSboeY7SPmYhdg fVrfq3HoGMCJFwoxm6Lx.

94 Dustin Voltz, “In Secret Meeting, China Acknowledged Role in U.S. Infrastructure Hacks,” The Wall Street Journal, April 10, 2025, archived April 18, 2025, https: //archive. is/nsLpC.

95 Simon Handler, "The 5×5—China’s cyber operations," The Atlantic Council, January 30, 2023, accessed May 6, 2025, https: //www. atlanticcouncil. org/content-series/the-5×5/the-5×5-chinas-cyber-operations/.

96 Gary Busch "Organised Crime in Asia – An [In]convenient Relationship: Part 2," Lima Charlie, February 24, 2019, accessed May 6, 2025, https: //limacharlienews. com/asia/organised-crime-in-asia-part-2/.

97 Lily Kuo, "Hong Kong: why thugs may be doing the government’s work," The Guardian, July 23, 2019, accessed May 6, 2025, https: //www. theguardian. com/world/2019/jul/22/ why-hong-kong-thugs-may-be-doing-the-governments-work.

98 “Beijing’s Ties to Organized Crime Undermine Democracies and Threaten Regional Stability,” IP Defense Forum, February 4, 2022, accessed May 22, 2025, https: //ipdefenseforum. com/2022/02/ gangsterism-with-chinese-characteristics/.

99 "APT41, A Dual Espionage and Cyber Crime Operation," Mandiant, 2022, accessed May 5, 2025, https: // services. google. com/fh/files/misc/apt41-a-dual-espionage-and-cyber-crime-operation. pdf.

100 "APT41, A Dual Espionage and Cyber Crime Operation," FireEye, archived, accessed May 5, 2025, https: //web. archive. org/web/20191213124611/https://content. fireeye. com/apt-41/rpt-apt41/.

101 Dake Kang and Zen Soo, “Leak lifts lid on Chinese hacking company – a sordid culture fuelled by alcohol and sex,” Independent, March 8, 2024, accessed May 6, 2025, https: //www. independent. co .uk/asia/ east-asia/i-soon-china-hacking-documents-b2509300. html.

102 Sebastian Rotella, "Outlaw Alliance: How China and Chinese Mafias Overseas Protect Each Other’s Interests," ProPublica, July 12, 2023, accessed May 6, 2025, https: //www. propublica. org/article/ how-beijing-chinese-mafia-europe-protect-interests.

103 “Gangsterism with Chinese Characteristics,” Indo-Pacific Defense Forum, February 4, 2022, accessed May 6, 2025, https: //ipdefenseforum. com/2022/02/ gangsterism-with-chinese-characteristics/.

104 Daniel Engel et al., “Can the United States Deter Threats from Uncertain Origins,” RAND, 2023, accessed May 6, 2025, https: //www. rand. org/content/dam/rand/pubs/research_reports/RRA1500/RRA1598-1/RAND_RRA1598-1. pdf.

105 Albert Zhang and Danielle Cave, "China’s cyber interference and transnational crime groups in Southeast Asia," The Strategist, July 24, 2023, accessed May 6, 2025, https: //www. aspistrategist. org. au/chinas-cyber-interference-and-transnational-crime-groups-in-southeast-asia/.

106 Albert Zhang and Danielle Cave, "China’s cyber interference narrows in on Australian politics and policy," ASPI, July 24, 2023, accessed May 6, 2025, https: //www. aspistrategist. org. au/chinas-cyber-interference-narrows-in-on-australian-politics-and-policy/.

107 “#StopRansomware: BianLian Ransomware Group,” CISA, last modified November 20, 2024, accessed May 6, 2025, https: //www. cisa. gov/news-events/cybersecurity-advisories/aa23-136a.

108 Andew Greene, “Rare earths miner targeted in cyber attack prior to removal of Chinese investors,” ABC News, June 4, 2024, accessed May 6, 2025, https: //www. abc. net. au/news/2024-06-04/rare-earths-miner-targeted-in-cyber-attack/103934020.

109 Paul Smith et al., “Rare earths miner hacked after Chinese investors ordered out,” Financial Review, June 4, 2024, accessed May 6, 2025, https: //www. afr. com/technology/rare-earths-miner-hacked-after-chinese-investors-ordered-out-20240604-p5jj8v.

110 “Same Cloak, More Dagger: Decoding How the People’s Republic of China Uses Cyberattacks,” Booz Allen Hamilton, 2022, accessed May 6, 2025, https: //www. boozallen. com/content/dam/home/pdf/natsec/china-cyber-report. pdf.

111 “AIIMS server outage being probed as ‘cyber terrorism’: Delhi Police,” Hindustan Times, November 24, 2022, accessed May 6, 2025, https: //www. hindustantimes. com/cities/delhi-news/aiims-server-outage-being-probed-as-cyber-terror-act-delhi-police-101669308187997. html.

112 Aleksandar Milenkoski and Julian-Ferdinand Vögele, "ChamelGang & Friends | Cyber espionage Groups Attacking Critical Infrastructure with Ransomware," SentinelOne, June 26, 2024, accessed May 6, 2025, https: //www. sentinelone. com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/.

113 Still Hsu and Zih-Cing Liao, "Unmasking CamoFei: An In-depth Analysis of an Emerging APT Group Focused on Healthcare Sectors in East Asia," TeamT5, August 19, 2023, accessed May 22, 2025, https: //stillu. cc/assets/slides/2023-08-Unmasking%20CamoFei. pdf.

114 Arvind Gunasekar, “"AIIMS Delhi Servers Were Hacked By Chinese, Damage Contained: Sources,” NDTV, December 14, 2022, accessed May 6, 2025, https: //www. ndtv. com/india-news/aiims-delhi-server-attack-was-by-chinese-5-physical-servers-infiltrated-by-hackers-data-retrieved-now-government-sources-3605639.

115 Aleksandar Milenkoski and Julian-Ferdinand Vögele, "ChamelGang & Friends | Cyber espionage Groups Attacking Critical Infrastructure with Ransomware," SentinelOne, June 26, 2024, accessed May 6, 2025, https: //www. sentinelone. com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/.

116 "Despite thriving trade, China’s relationship with Brazil is weakening," The Economist, February 12, 2022, accessed May 6, 2025, https: //archive. is/tuxNz.

117 Tom Madjar, “The Malware That Must Not Be Named: Suspected Espionage Campaign Delivers ‘Voldemort’,” Proofpoint, last modified October 22, 2024, accessed May 6, 2025, https: //www. proofpoint. com/us/blog/threat-insight/malware-must-not-be-named-suspected-espionage-campaign-delivers-voldemort.

118 "The Chinese groups accused of hacking the US and others," Reuters, July 21, 2023, accessed May 6, 2025, https: //www. reuters. com/world/china/chinese-groups-accused-hacking-us-others-2023-07-21/.

119 “Silk Typhoon targeting IT supply chain,” Microsoft, March 5, 2025, accessed May 6, 2025, https: //www. microsoft. com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/.

120 Steve Holland and Dolna Chlacu, "U.S. and allies accuse China of global hacking spree," Reuters, July 20, 2021, accessed May 6, 2025, https: //www. reuters. com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19/.

121 Zhang Han, “China urges US to stop politicizing cybersecurity issues: Five Eyes carefully plot, coordinate in smear campaign,” Global Times, March 26, 2024, accessed May 6, 2025, https: //www. globaltimes. cn/page/202403/1309549. shtml.

122 “APT40 Advisory,” Australian Signals Directorate, July 9, 2024, accessed May 6, 2025, https: //www. cyber. gov. au/about-us/view-all-content/alerts-and-advisories/apt40-advisory-prc-mss-tradecraft-in-action.

123 Matt Burgess, “The Mystery of China’s Sudden Warnings About US Hackers,” Wired, May 26, 2022, accessed May 6, 2025, https: //archive. is/DDRb7.

124 China Blames US Intelligence Agencies for Earthquake Centre Cyber Attack,” Australian Cybersecurity Magazine, August 18, 2023, accessed May 6, 2025, https: //australiancybersecuritymagazine. com. au/china-blames-us-intelligence-agencies-for-earthquake-centre-cyber-attack/.

[125] Lina Lau, “An inside look at NSA (Equation Group) TTPs from China’s lense,” Inversecos, February 18, 2025, accessed May 6, 2025, https: //www. inversecos. com/2025/02/an-inside-look-at-nsa-equation-group. html.

[126] “Investigation Report on the US Cyberattack Against a Chinese Advanced Materials Research Institute [美网络攻击我国某先进材料设计研究院事件调查报告],” CNCERT, January 17, 2025, archived January 21, 2025, https: //archive. is/pqel5.

[127] “CNCERT handles two U.S. cyberattacks targeting major Chinese tech firm, institution,” Global Times, December 18, 2024, accessed May 6, 2025, https: // archive. is/6RIUl.

[128] “Foreign Ministry Spokesperson Lin Jian’s Regular Press Conference on March 26, 2024,” Embassy of the People’s Republic of China in the United States of America, March 26, 2024, accessed May 6, 2025, http: //us. china-embassy. gov. cn/eng/fyrth/202403/t20240326_11271172. htm.

[129] “China rejects accusations it targeted US Treasury in cyberattack,” France24, December 31, 2024, accessed May 6, 2025, https: //www. france24. com/en/americas/20241231-china-rejects-accusations-it-targeted-us-treasury-in-cyberattack.

[130] Andrew Methven, “A thief crying “stop thief!” — phrase of the week,” The China Project, May 20, 2022, accessed May 6, 2025, https: //thechinaproject. com/2022/05/20/a-thief-crying-stop-thief-phrase-of-the-week/.

[131] “Playing ‘a-thief-crying-stop-thief’ trick, US only wants ‘permanent cyber hegemony’,” Global Times, September 20, 2023, accessed May 6, 2025, https: // www. globaltimes. cn/page/202309/1298564. shtml.

[132] Liu Caiyu, “US practices 'thief crying stop thief,' says Chinese FM on indictment of 12 Chinese nationals over alleged cyberattacks,” Global Times, March 6, 2025, accessed May 6, 2025, https: //www. globaltimes. cn/page/202503/1329596. shtml.

[133] “China firmly rejects US accusations about hacking,” Global Times, April 8, 2022, accessed May 6, 2025, https: //www. globaltimes. cn/page/202204/1258859. shtml.

[134] Matt Burgess, “The Mystery of China’s Sudden Warnings About US Hackers,” Wired, May 26, 2022, accessed May 6, 2025, https: //archive. is/DDRb7.

[135] "Spokesperson’s Remarks on Report Revealing Truths of US Hyping up of 'Volt Typhoon'," PRC Ministry of Foreign Affairs, last modified October 15, 2024, archived December 7, 2024, https: //web. archive. org/web/20241207235922/https: //www. mfa. gov. cn/eng/wjb/zzjg_663340/jks_665232/jkxw_665234/202410/t20241015_11507722. html/.

[136] "Spokesperson’s Remarks on Report Revealing Truths of US Hyping up of 'Volt Typhoon'," PRC Ministry of Foreign Affairs, last modified October 15, 2024, archived December 7, 2024, https: //web. archive. org/web/20241207235922/https: //www. mfa. gov. cn/eng/wjb/zzjg_663340/jks_665232/jkxw_665234/202410/t20241015_11507722. html/.

[137] Zhao Siwei, “"Exclusive: Evidence shows US’ NSA behind attack on email system of leading Chinese aviation university,” last modified September 5, 2022, accessed May 9, 2025, https: //www. globaltimes. cn/page/202209/1274627. shtml.

[138] “National Security Agency Announces Retirement of Cybersecurity Director,” National Security Agency, February 20, 2024, accessed May 9, 2025, https: // www. nsa. gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3681065/national-security-agency-announces-retirement-of-cybersecurity-director/.

[139] “Rob Joyce,” Enigma, n.d., accessed archived July 15, 2017, https: //web. archive. org/web/20170715062208/https: //www. usenix. org/conference/enigma2016/speaker-or-organizer/rob-joyce-chief-tailored-access-operations-national.

[140] Yuan Hong, “Identity of NSA hacker behind cyberattack on China's leading aviation university identified; to be disclosed in due course: source,” Global Times, last modified September 14, 2023, accessed May 9, 2025, https: //www. globaltimes. cn/page/202309/1298164. shtml.

[141] Alex Joske, “The China Defence Universities Tracker,” Australian Strategic Policy Institute, November 25, 2019, accessed May 9, 2025, https: //www. aspi. org. au/report/china-defence-universities-tracker.

[142] “Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections,” Google - Mandiant, October 22, 2022, accessed May 30, 2025, https: //cloud. google. com/blog/topics/threat-intelligence/prc-dragonbridge-influence-elections.

[143] “国安部公开4名“台独”网军身份信息 [Ministry of State Security Publishes Identities of Four “Taiwan Independence” Cyber Operatives],” CCTV News, March 17, 2025, accessed May 9, 2025, http: //photo. china. com. cn/2025-03/17/content_117769597. shtml.

[144] Li Weichao, “Profiles of 4 cyberattackers related to 'Taiwan independence' forces disclosed,” China Daily, March 17, 2025, accessed May 9, 2025, http: //eng. chinamil. com. cn/CHINA_209163/TopStories_209189/16375389. html.

[145] “低技术武器+持久战策略：台湾黑客组织18年来对大陆网络攻击实录, [Low-Tech Weapons + War of Attrition Strategy: An 18-Year Record of Cyberattacks Against Mainland China by a Taiwanese Hacker Group],” Qi An Xin Group, March 17, 2025, accessed May 9, 2025, https: //www. secrss. com/articles/76715.

[146] “台湾“绿斑”攻击组织使用开源远控木马的一组钓鱼攻击分析 [Analysis of a Phishing Campaign by Taiwan's "Green Spot" Attack Group Using Open-Source Remote Access Trojans],“ Antiy Lab, March 17, 2025, accessed May 9, 2025, https: //www. antiy. cn/research/notice&report/research_report/GreenSpot_Analysis_202503. html.

[147] “以“毒云藤”为例：“台独”势力网络间谍活动解析 [Using "Toxic Kudzu" as an Example: An Analysis of Cyber Espionage Activities by “Taiwan Independence” Forces],” ShadowLab Cybersecurity, March 17, 2025, accessed May 9, 2025, https: //mp. weixin. qq. com/s/3nPKv9Dzre3f1MCSsmyCvA.

[148] Guo Yuandan, “US conducts cyberattacks against major Chinese commercial encryption provider: report,” Global Times, April 28, 2025, accessed May 9, 2025, https: //www. globaltimes. cn/page/202504/1333032. shtml.

[149] “悬赏通缉！3名美国特工对亚冬会实施网攻窃密被锁定 [Wanted! 3 U.S. Agents Identified for Cyberattacks and Espionage Targeting the Asian Winter Games],” China Daily, April 15, 2025, accessed May 9, 2025, https: //cn. chinadaily. com[.]cn/a/202504/15/WS67fdb569a310e29a7c4a914a. html.

[150] “Cyber Threat Report of The 9th Asian Winter Games Harbin 2025,” National Computer Virus Emergency Response Center, April 3, 2025, accessed May 9, 2025, https: //www. cverc. org. cn/head/zhaiyao/Cyber_Threat_Report_of_The_9th_Asian_Winter_Games_Harbin_2025_EN. pdf.

[151] “城市侧网络安保中的高频事件案例分析 [Analysis of High-Frequency Incident Cases in Urban Cybersecurity Protection],” AnTian Group, April 14, 2025, accessed May 9, 2025, https: //mp. weixin. qq. com/s/0a4ggqNJ5HG5Tg5xTmCWpw.

[152] Zhao Jia, “China urges US to stop targeted cyberattacks,” China Daily, last modified April 15, 2025, accessed May 9, 2025, https: //www. chinadaily. com. cn/a/202504/15/WS67fe1bf7a3104d9fd381f6f0. html.

[153] Dylan Welch, “Taiwan’s Election: 2024’s Canary in the Coal Mine for Disinformation against Democracy,” DMG, December 19, 2023, accessed May 9, 2025, https: //www. gmfus. org/news/taiwans-election-2024s-canary-coal-mine-disinformation-against-democracy.

[154] Emily Feng, “Taiwan deals with lots of misinformation, and it's harder to track down,” NPR, January 11, 2024, accessed May 9, 2025, https: //www. npr. org/2024/01/11/1216340756/taiwan-election-disinformation-social-media-ptt.

[155] “Targeting Taiwan: China’s influence efforts on the island,” DFR Lab, May 6, 2024, accessed May 9, 2025, https: //dfrlab. org/2024/05/06/targeting-taiwan-chinas-influence-efforts-on-the-island/.

[156] “Taiwan election: when the chips are down,” Tech Informed, January 13, 2024, accessed May 9, 2025, https: //techinformed. com/taiwan-election-when-the-chips-are-down/.

[157] Emily Feng, “Taiwan deals with lots of misinformation, and it's harder to track down,” NPR, January 11, 2024, accessed May 9, 2025, https: //www. npr. org/2024/01/11/1216340756/taiwan-election-disinformation-social-media-ptt.

[158] Sana Hashmi, “Taiwan should welcome Indians,” Taipei Times, November 21, 2023, accessed May 9, 2025, https: //www. taipeitimes. com/News/editorials/archives/2023/11/21/2003809467.

[159] “NHK film exposes cyberattacks against Taiwan,” Taipei Times, October 22, 2024, accessed May 9, 2025, https: //www. taipeitimes. com/News/taiwan/archives/2024/10/22/2003825680.

[160] “Targeting Taiwan: China’s influence efforts on the island,” DFR Lab, May 6, 2024, accessed May 9, 2025, https: //dfrlab. org/2024/05/06/targeting-taiwan-chinas-influence-efforts-on-the-island/.

[161] “Man held for allegedly faking election surveys,” Liberty Times, December 24, 2023, accessed May 9, 2025, https: //news. ltn. com. tw/news/focus/breakingnews/4530234.

[162] “How to Succeed at Annexation Without Really Fighting,” Booz Allen Hamilton, 2024, accessed May 6, 2025, https: //www. boozallen. com/content/dam/home/pdf/cyber/national-cyber-how-to-succeed-at-annexation-without-fighting. pdf, p. 34.

[163] “China steps up disinformation campaign in 2024: NSB report,” Overseas Community Affairs Council, January 5, 2025, accessed May 9, 2025, https: //www. ocac. gov. tw/OCAC/Eng/Pages/Detail. aspx?nodeid=329&pid=71573982.

[164] Yimou Lee, “Chinese cyberattacks on Taiwan government averaged 2.4 mln a day in 2024, report says,” last modified January 6, 2025, accessed May 9, 2025, https: //www. reuters. com/technology/cybersecurity/chinese-cyberattacks-taiwan-government-averaged-24-mln-day-2024-report-says-2025-01-06/.

[165] “Daily cyberattacks on Taiwan government double in 2024: NSB,” Focus Taiwan, January 5, 2025, accessed May 9, 2025, https: //focustaiwan. tw/cross-strait/202501050011.

[166] “信息优势的度量 [Measuring Information Superiority],” People’s Daily, March 17, 2015, accessed May 9, 2025, http: //military. people. com. cn/n/2015/0317/c172467-26702265. html.

[167] “Ransomware Group: Crazyhunter,” Ransomware Live, n.d., archived April 11, 2025, https: //archive. is/H3UO7.

[168] Charlotte Lee, “Taiwan warns of 3 fraud scams after hospital data leaks,” Taiwan News, March 11, 2025, accessed May 9, 2025, https: //www. taiwannews. com. tw/news/6056408.

[169] Michael Nakhiengchanh, "Taipei’s Mackay Memorial Hospital faces ransomware attack," Taiwan News, February 11, 2025, accessed May 9, 2025, https: //taiwannews. com. tw/news/6034795.

[170] Hu Xinnan, “Chinese hacker wanted for blackmailing Mackay Memorial Hospital,” Yahoo News, April 2, 2025, accessed May 19, 2025, https: //tw. news. yahoo. com陸駭客勒索馬偕醫院-遭通緝-201000592.htm.

[171] “Chinese hacker targeting hospital identified: police¸” Taiwan Times, April 3, 2025, accessed May 19, 2025, https: //www. taipeitimes. com/News/front/archives/2025/04/03/2003834526.

[172] “The Chinese Communist Party has combined cyberattacks with cybercrime tactics. For example, the healthcare sector has recently suffered successive ransomware attacks, and hackers have sold the stolen data on forums and leveraged the effect of media dissemination to spread it further., attempting to impact the stability of people’s livelihoods and social order in our country.” Statement by Taiwan’s National Security Bureau Director-General, Tsai Ming-yen, at the Legislative Yuan on April 8, 2025, accessed May 19, 2025, https: //ppg. ly. gov. tw/ppg/SittingAttachment/download/2025040112/10834825000010021002. pdf.

[173] Joey Chen et al., “APT41 likely compromised Taiwanese government-affiliated research institute with ShadowPad and Cobalt Strike,” Talos, August 1, 2024, accessed May 9, 2025, https: //blog. talosintelligence. com/chinese-hacking-group-apt41-compromised-taiwanese-government-affiliated-research-institute-with-shadowpad-and-cobaltstrike-2/.

[174] “Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation,” Recorded Future, June 24, 2024, accessed May 9, 2025, https: //go. recordedfuture. com/hubfs/reports/cta-cn-2024-0624. pdf.

[175] Pierre Lee and Vickie Su, "TIDRONE Targets Military and Satellite Industries in Taiwan," TrendMicro, September 5, 2024, accessed May 29, 2025, https: //www. trendmicro. com/en_us/research/24/i/tidrone-targets-military-and-satellite-industries-in-taiwan. html.

[176] Joey Chen, “Lotus Blossom espionage group targets multiple industries with different versions of Sagerunex and hacking tools,” February 27, 2025, accessed May 9, 2025, https: //blog. talosintelligence. com/lotus-blossom-espionage-group/.

[177] “Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific,” Unit 42, November 17, 2023, accessed May 9, 2025, https: //unit42. paloaltonetworks. com/stately-taurus-targets-philippines-government-cyber espionage/.

[178] Jim Gomez and Aaron Favila, "Philippine supply boats breach a Chinese coast guard blockade in the hotly contested South China Sea," Associated Press, last modified August 24, 2023, accessed May 9, 2025, https: //apnews. com/article/south-china-sea-disputes-philippines-b7a110ca593f502759b690a3cf071912.

[179] “Philippines wards off cyber attacks from China-based hackers,” Straits Times, February 5, 2024, accessed May 9, 2025, https: //www. straitstimes. com/asia/philippines-wards-off-cyber-attacks-from-china-based-hackers.

[180] Jamie Tarabay, “Chinese Hackers Target Philippine President, Steal Military Data,” Bloomberg, January 7, 2025, archived January 7, 2025, https: //archive. is/gelzZ.

[181] Jeoffrey Maitem, “Philippines steps up defences against Chinese hackers after ‘cyberwar’ warning from telecoms security chief,” South China Morning Post, last modified April 10, 2025, archived, April 6, 2025, https: //archive. is/YVw8q.

[182] Albert Zhang, “China’s high stakes and deepfakes in the Philippines,” The Strategist, August 2, 2024, accessed May 9, 2025, https: //www. aspistrategist. org.au/chinas-high-stakes-and-deepfakes-in-the-philippines/.

[183] “US exploits hacking allegations to stir up tensions in South China Sea,” Global Times, January 9, 2025, accessed May 9, 2025, https: //www. globaltimes. cn/page/202501/1326621. shtml.

[184] Ryan Tomcik, “Always Another Secret: Lifting the Haze on China-nexus Espionage in Southeast Asia,” Google Cloud, November 28, 2022, accessed May 9, 2025, https: //cloud. google. com/blog/topics/threat-intelligence/china-nexus-espionage-southeast-asia/.

[185] Bea Cupin, “In Manila, how China set up an influence, espionage network,” Rappler, August 10, 2024, accessed May 9, 2025, https: //www. rappler. com/newsbreak/investigative/how-china-set-up-influence-espionage-network-manila/.

[186] Ted Lee and Hara Hiroaki, “Attack on Security Titans: Earth Longzhi Returns With New Tricks,” Trend Micro, May 2, 2023, accessed May 9, 2025, https: //www. trendmicro. com/en_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks. html.

[187] “NBI ARRESTS ONE CHINESE NATIONAL AND TWO FILIPINOS FOR ILLEGAL SURVEILLANCE AND SPYING ACTIVITIES,” Leader News Philippines, January 20, 2025, accessed May 9, 2025, https: //www. facebook. com/leadernews. ph/posts/nbi-arrests-one-chinese-national-and-two-filipinos-for-illegal-surveillance-and-/1053378210156340/.

[188] “MirrorFace によるサイバー攻撃について [Regarding Cyberattacks by MirrorFace], National Police Agency - Cabinet Cybersecurity Center, January 8, 2025, accessed May 9, 2025, https: //www. npa. go. jp/bureau/cyber/pdf/20250108_caution. pdf.

[189] “210 hacks made on JAXA, other Japan targets by China group since 2019,” The Mainichi, January 8, 2025, accessed May 9, 2025, https: //web. archive. org/web/20250111090658/https: //mainichi. jp/english/articles/20250108/p2g/00m/0sc/033000c.

[190] “Cuckoo Spear – the latest Nation-state Threat Actor targeting Japanese companies,” Cybereason, n.d., accessed May 9, 2025, https: //www. cybereason. com/blog/cuckoo-spear.

191 Shusei Tomonaga, “攻撃グループMirrorFaceの攻撃活動 [Attack Activities of the Hacker Group MirrorFace],” JPCERT, August 9, 2024, accessed May 9, 2025, https: //blogs. jpcert. or. jp/ja/2024/07/mirrorface. html.

192 Mari Yamaguchi, “Japan links Chinese hacker MirrorFace to dozens of cyberattacks targeting security and tech data,” Associated Press, last modified January 8, 2025, accessed May 9, 2025, https: //apnews. com/article/japan-police-cyberattack-china-government-68adcb293b2931da4c30ca0279720124.

193 RevivalStone：Winnti Groupによる日本組織を狙った攻撃キャンペーン [RevivalStone: An Attack Campaign Targeting Japanese Organizations by the Winnti Group Security],” LAC, February 13, 2025, accessed May 9, 2025, https: //www. lac. co. jp/lacwatch/report/20250213_004283. html.

194 “People's Republic of China-Linked Cyber Actors Hide in Router Firmware,” National Security Agency et al., September 2023, accessed May 9, 2025, https: //media. defense. gov/2023/Sep/27/2003309107/-1/-1/0/CSA_BLACKTECH_HIDE_IN_ROUTERS_TLP-CLEAR. PDF.

195 “Operation Blotless攻撃キャンペーンに関する注意喚起 [Security Alert Regarding the Operation Blotless Attack Campaign],” JPCERT June 25, 2024, accessed May 9, 2025, https: //www. jpcert. or. jp/at/2024/at240013. html.

196 “Operation Blotless攻撃キャンペーンに関する注意喚起 [Security Alert Regarding the Operation Blotless Attack Campaign],” Deiwa Institute of Research, n.d., accessed May 9, 2025, https: //www. dir. co. jp/report/technology/security/20241009_024646. pdf.

197 Hara Hiroaki, “Guess Who’s Back - The Return of ANEL in the Recent Earth Kasha Spear-phishing Campaign in 2024,” TrendMicro, November 26, 2024, accessed May 9, 2025, https: //www. trendmicro. com/en_us/research/24/k/return-of-anel-in-the-recent-earth-kasha-spearphishing-campaign. html.

198 Shusei Tomonaga, “Recent Cases of Watering Hole Attacks, Part 2,” JPCERT, December 26, 2024, accessed May 9, 2025, https: //blogs. jpcert. or. jp/en/2024/12/watering_hole_attack_part2. html.

199 Mari Yamaguchi, “Japan links Chinese hacker MirrorFace to dozens of cyberattacks targeting security and tech data,” Associated Press, last modified January 8, 2025, accessed May 9, 2025, https: //apnews. com/article/japan-police-cyberattack-china-government-68adcb293b2931da4c30ca0279720124.

200 “Pro-China group may be behind breach of Japan govt. cybersecurity center,” NHK World – Japan, August 5, 2023, archived August 5, 2023, https: //web. archive. org/web/20230805082049/https: //www3. nhk. or. jp/nhkworld/en/news/20230805_09/.

201 Austin Larsen, “Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868),” Google Cloud, August 29, 2023, accessed May 9, 2025, https: //cloud. google. com/blog/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation.

202 Leo Lewis, “Japan’s cyber security agency suffers months-long breach,” The Financial Times, August 29, 2023, archived September 14, 2023, https: //archive. is/r5wRY.

203 Ali Mammadov, “Opinion – Weakened US Relations Is Pushing Europe Towards China,” E-International Relations, April 6, 2025, accessed May 9, 2025, https: //www. e-ir. info/2025/04/06/opinion-weakened-us-relations-is-pushing-europe-towards-china/.

204 Daniel Hamilton, “Coming Together or Falling Apart Over China?,” CEPA, January 30, 2025, accessed May 9, 2025, https: //cepa. org/commentary/coming-together-or-falling-apart-over-china/.

205 Maria Papageorgiou and Zeno Leoni, “The Five Eyes Allies and China: Assessing Threat Perceptions and Power Dynamics,” Journal of Chinese Political Science, April 14, 2025, accessed May 9, 2025, https:/ /link. springer. com/article/10. 1007/s11366-025-09913-w.

206 “Mustang Panda Uses the Russian-Ukrainian War to Attack Europe and Asia Pacific Targets,” BlackBerry, December 6, 2022, accessed May 9, 2025, https: //blogs. blackberry. com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets.

207 “Mustang Panda APT Group Uses European Commission-Themed Lure to Deliver PlugX Malware,” ElasticIQ, February 2, 2023, accessed May 9, 2025, https: //blog. eclecticiq. com/mustang-panda-apt-group-uses-european-commission-themed-lure-to-deliver-plugx-malware.

208 “Chinese Threat Actors Targeting Europe in SmugX Campaign,” Check Point Research, July 3, 2023, accessed May 9, 2025, https: //research. checkpoint. com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/.

209 Alexandre Côté Cyr, "MQsTTang: Mustang Panda’s latest backdoor treads new ground with Qt and MQTT," ESET, March 2, 2023, accessed May 9, 2025, https: //www. welivesecurity. com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt/.

210 Asheer Malhotra et al., “Mustang Panda deploys a new wave of malware targeting Europe,” Talos, May 5, 2022, accessed May 9, 2025, https: //blog. talosintelligence. com/mustang-panda-targets-europe/.

211 “SmugX: Unveiling a Chinese-Based APT Operation Targeting European Governmental Entities: Check Point Research Exposes a Shifting Trend,” Check Point, July 3, 2023, accessed May 9, 2025, https: //blog. checkpoint. com/securing-user-and-access/smugx-unveiling-a-chinese-based-apt-operation-targeting-european-governmental-entities-check-point-research-exposes-a-shifting-trend/.

212 K.Z., “Znano, kdo stoji za napadom na ministrstvo za zunanje zadeve [It is known who is behind the attack on the Ministry of Foreign Affairs],” Zurnal 24, April 12, 2023, accessed May 9, 2025, https: //www. zurnal24. si/slovenija/znano-kdo-stoji-za-napadom-na-ministrstvo-za-zunanje-zadeve-404450.

213 “New details emerge about cyberattack on Foreign Ministry,” Slovenia Times, April 26, 2023, accessed May 9, 2025, https: //sloveniatimes. com/38169/new-details-emerge-about-cyberattack-on-foreign-ministry.

214 Chetan Raghuprasad and Ashley Shen, “SneakyChef espionage group targets government agencies with SugarGh0st and more infection techniques,” Cisco Talos, June 21, 2024, accessed May 9, 2025, https: //blog. talosintelligence. com/sneakychef-sugargh0st-rat/.

215 William Yang, “Taiwan Seeks Deeper Relations with Baltic States Despite Chinese Opposition,” VOA, November 9, 2023, accessed May 9, 2025, https: //www. voanews. com/a/taiwan-seeks-deeper-relations-with-baltic-states-despite-chinese-opposition-/7348081. html.

216 “IISS Prague Defense Summit 2024: Speaker Agenda,” IISS, n.d., accessed May 9, 2025, https: //www. iiss. org/events/prague-defence-summit/prague-defence-summit-2024/speaker-agenda/.

217 Ilaria Mazzocco and Andrea Leonard Palazzi, “Italy Withdraws from China’s Belt and Road Initiative,” CSIS, December 14, 2023, accessed May 9, 2025, https: //www. csis. org/analysis/italy-withdraws-chinas-belt-and-road-initiative.

218 David Sakes, “Why Is Italy Withdrawing From China’s Belt and Road Initiative?,” Council on Foreign Relations, August 3, 2023, accessed May 9, 2025, https: //www. cfr. org/blog/why-italy-withdrawing-chinas-belt-and-road-initiative.

219 Ted Lee and Theo Chen, “A Dive into Earth Baku’s Latest Campaign,” TrendMicro, August 9, 2024, accessed May 9, 2025, https: //www. trendmicro. com/en_us/research/24/h/earth-baku-latest-campaign. html.

220 “Uncovering an undetected KEYPLUG implant attacking Italian Industries,” Tinexta Cyber, n.d., accessed May 9, 2025, https: //www. tinextacyber. com/wp-content/uploads/2024/07/2405-APT41-KeyplugReport-2. pdf.

221 Mike Stokkel et al., “APT41 Has Arisen From the DUST,” Google Cloud, July 18, 2024, accessed May 9, 2025, https: //cloud. google. com/blog/topics/threat-intelligence/apt41-arisen-from-dust.

222 “Uncovering an undetected KEYPLUG implant attacking Italian Industries,” Tinexta Cyber, n.d., accessed May 9, 2025, https: //www. tinextacyber. com/wp-content/uploads/2024/07/2405-APT41-KeyplugReport-2. pdf.

223 Tommy Madjar et al., “The Malware That Must Not Be Named: Suspected Espionage Campaign Delivers ‘Voldemort,’” Proofpoint, August 29, 2024, accessed May 9, 2025, https: //www. proofpoint. com/us/blog/threat-insight/malware-must-not-be-named-suspected-espionage-campaign-delivers-voldemort.

224 Giulia Pompili, “La fabbrica dei contenuti pro Cina [The Pro-China Content Factory],” Il Foglio, October 25, 2023, accessed May 9, 2025, https: //www. ilfoglio. it/esteri/2023/10/25/news/la-fabbrica-dei-contenuti-pro-cina-5826677/amp/.

225 “Network of fake, pro-China “news” websites unveiled in Italy,” Decode39, October 25, 2023, accessed May 9, 2025, https //decode39. com/8109/network-fake-china-news-websites-italy/.

226 Joshua Sullivan and Jon Bateman, “China Decoupling Beyond the United States: Comparing Germany, Japan, and India,” Carnegie Endowment for International Peace, January 8, 2025, accessed May 9, 2025, https: //carnegieendowment. org/research/2025/01/china-decoupling-beyond-the-united-states-comparing-germany-japan-and-india?lang=en.

227 Ido Vock, “Germany spying: Three suspected Chinese agents arrested,” BBC, April 22, 2024, accessed May 9, 2025, https: //www. bbc. com/news/world-europe-68873836.

228 “The German Chancellor Presses China on Russia's Invasion of Ukraine,” The Associated Press, April 16, 2025, accessed May 9, 2025, https: //www. usnews. com/news/business/articles/2024-04-16/on-a-china-visit-the-german-chancellor-says-russias-invasion-of-ukraine-threatens-global-security.

229 Ted Lee et al., “Breaking Down Earth Estries' Persistent TTPs in Prolonged Cyber Operations,” TrendMicro, November 8, 024, accessed May 9, 2025, https: //www. trendmicro. com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o. html/.

230 “APT Activity Report,” ESET, 2024, accessed May 9, 2025, https: //web-assets. esetstatic. com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2023-q1-2024. pdf.

231 “APT Activity: WIPERS, PHISHING, AND UNPATCHED VULNERABILITIES October 2024 – March 2025 Report,” ESET, May 19, 2025, accessed May 19, 2025, https: //web-assets. esetstatic. com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2024-q1-2025. pdf.

232 Nick Chubb et al., “The Great Disconnect,” Thetius et al., n.d., accessed May 9, 2025, https: //cyberowl. io/wp-content/uploads/2022/04/CyberOwl-HFW-Thetius-Cyber-Security-Report-The-Great-Disconnect-. pdf.

233 Elaine Dezenski and David Rader, “How China Uses Shipping for Surveillance and Control,” Foreign Policy, September 20, 2023, accessed May 9, 2025, https: //foreignpolicy. com/2023/09/20/china-shipping-maritime-logistics-lanes-trade-ports-security-espionage-intelligence/.

234 Andy Greenberg, “How a Shady Chinese Firm’s Encryption Chips Got Inside the US Navy, NATO, and NASA,” Wired, June 15, 2023, accessed May 9, 2025, https: //www. wired. com/story/hualan-encryption-chips-entity-list-china/.

235 “Addition of Certain Entities to the Entity List; Revision of ...,” Federal Register, July 12, 2021, accessed May 9, 2025, https: //www. federalregister. gov/documents/2021/07/12/2021-14656/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entry-on-the-entity-list.

236 “PRC-Linked Disinformation Claims Conservatives Threaten Chinese Diaspora Interests, Aims at PM Carney’s Debate Remark,” The Bureau, April 18, 2025, accessed May 9, 2025, https: //www. thebureau. news/p/prc-linked-disinformation-claims.

237 Fitriani and Nira Calwyn, “China targets Canada’s election—and may be targeting Australia’s,” Australian Strategic Policy Institute, April 16, 2025, accessed May 9, 2025, https: //www. aspistrategist. org. au/china-targets-canadas-election-and-may-be-targeting-australias/.

238 Stephanie Taylor et al., “CSIS prepped PMO briefing on China's election meddling, documents at inquiry show,” The Canadian Press, last modified April 8, 2024, accessed May 9, 2025, https: //thecanadianpressnews. ca/national/csis-prepped-pmo-briefing-on-chinas-election-meddling-documents-at-inquiry-show/article_2f6c6b3b-a0de-54fe-8eae-0dd4a15411e3. html.

239 Liu Xin, “Mark Carney to succeed Trudeau as PM, warns US not to make mistake as Canada will win trade war,” The Global Times, March 10, 2025, accessed May 9, 2025, https: //www. globaltimes. cn/page/202503/1329820.shtml.

240 Darren Major, “6 big moments and takeaways from the final leaders' debate,” CBC, last modified April 18, 2025, accessed May 9, 2025, https: //www. cbc. ca/news/politics/key-moments-english-leadership-debate-1.7513787.

241 Fitriani and Nira Calwyn, “China targets Canada’s election—and may be targeting Australia’s,” Australian Strategic Policy Institute, April 16, 2025, accessed May 9, 2025, https: //www. aspistrategist. org. au/china-targets-canadas-election-and-may-be-targeting-australias/.

242 Albert Zhang and Danielle Cave, “China’s cyber interference narrows in on Australian politics and policy,” Australian Strategic Policy Institute, July 24, 2023, accessed May 9, 2025, https: //www. aspistrategist. org. au/chinas-cyber-interference-narrows-in-on-australian-politics-and-policy/.

243 Mark DeGeurin, “Salacious Chinese Disinformation Campaign Blames Maui Fires on Deadly American ‘Weather Weapon’,” Gizmodo, September 11, 2023, accessed May 9, 2025, https: //gizmodo. com/weather-weapon-maui-fires-china-disinformation-1850826548.

244 “Canada says China-linked 'Spamouflage' campaign targeted lawmakers, PM Trudeau,” Reuters, last modified October 23, 2023, accessed May 9, 2025, https: //www. reuters. com/world/canada-says-china-linked-spamouflage-campaign-targeted-lawmakers-pm-trudeau-2023-10-23/.

245 “Electoral Commission response to cyber-attack attribution,” The Electoral Commission, March 25, 2024, accessed May 9, 2025, https: //www. electoralcommission. org. uk/media-centre/electoral-commission-response-cyber-attack-attribution-0.

246 UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity,” UK Government, last modified April 2, 2024, accessed May 9, 2025, https: //www. gov. uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity.

247 Lucy Craymer, “New Zealand accuses China of hacking parliament, condemns activity,” Reuters, March 26, 2024, accessed May 9, 2025, https: //www. reuters. com/technology/cybersecurity/new-zealand-says-parliamentarian-entities-hit-2021-by-malicious-cyber-activity-2024-03-25/.

248 Adam Pearse, “GCSB spy agency knew China-backed cyber attack targeted former MPs and didn’t tell them,” New Zealand Herald, April 30, 2024, accessed May 9, 2025, https: //www. nzherald. co. nz/nz/politics/former-mps-angry-government-didnt-warn-them-they-were-targeted-in-china-backed-cyberattack/EBNYAK2G6BHIRDHZLLNJ5VHEXM/.

249 “National Cyber Threat Assessment: 2025-2026,” Canadian Centre for Cyber Security, n.d., accessed May 9, 2025, https: //www. cyber. gc. ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e. pdf.

250 Ellen Mirigan et al., “UK Fears Chinese Hackers Compromised Critical Infrastructure,” Bloomberg, October 15, 2024, archived October 14, 2024, https: //archive. is/i7tvj.

251 “People’s Republic of China activity targeting network edge routers: Observations and mitigation strategies,” Canadian Centre for Cyber Security, April 15, 2025, accessed May 9, 2025, https: //www. cyber. gc. ca/en/news-events/peoples-republic-china-activity-targeting-network-edge-routers-observations-mitigation-strategies.

252 “U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure,” U.S. Department of Justice, January 31, 2024, May 9, 2025, https: //www. justice. gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical.

253 “Volt Typhoon Compromises 30% of Cisco RV320/325 Devices in 37 Days,” SecurityScorecard, n.d., accessed May 9, 2025, https: //www. securityweek. tcom/wp-content/uploads/2024/01/Volt-Typhoon.pdf.

254 “KV-Botnet: Don’t call it a Comeback,” Lumen, February 7, 2024, accessed May 9, 2025, https: //blog. lumen. com/kv-botnet-dont-call-it-a-comeback/.

255 “Routers Roasting on an Open Firewall: the KV-botnet Investigation,” Lumen, December 13, 2023, accessed May 9, 2025, https: //blog. lumen. com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/.

256 Alex Forsyth, “MoD data breach: UK armed forces' personal details accessed in hack,” BBC, May 6, 2024, accessed May 9, 2025, https: //www. bbc. com/news/uk-68966497/.

257 Machael Raggi, “Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect,” Google Cloud, March 21, 2024, accessed May 9, 2025, https: //cloud. google. com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect.

258 Aparna Bharadwaj et al., “In a Multipolar World, the Global South Finds Its Moment,” Boston Consulting Group, April 22, 2025, accessed May 13, 2025, https: //www. bcg. com/publications/2025/in-a-multipolar-world-global-south-finds-its-moment.

259 Prashanth Parameswaran, “Rising Global South Discontent Amid Strategic Competition in the Indo-Pacific and Beyond,” Wilson Center, August 9, 2024, accessed May 13, 2025, https: //www. wilsoncenter. org/article/rising-global-south-discontent-amid-strategic-competition-indo-pacific-and-beyond.

260 Aaron Ross et al., “Exclusive: Chinese hackers attacked Kenyan government as debt strains grew,” Reuters, last modified May 24, 2023, accessed May 9, 2025, https: //www. reuters. com/world/africa/chinese-hackers-attacked-kenyan-government-debt-strains-grew-2023-05-24/.

261 “Chinese State-Sponsored RedDelta Targeted Taiwan, Mongolia, and Southeast Asia with Adapted PlugX Infection Chain,” Recorded Future, January 9, 2025, accessed May 9, 2025, https: //www. recordedfuture. com/research/reddelta-chinese-state-sponsored-group-targets-mongolia-taiwan-southeast-asia.

262 “Yearender: Ethiopia-China all-weather strategic partnership solidified in 2024,” Xinhua, December 28, 2024, accessed May 9, 2025, http: //www. china. org. cn/world/Off_the_Wire/2024-12/28/content_117633580.htm.

263 Chetan Raghuprasad and Ashley Shen, “SneakyChef espionage group targets government agencies with SugarGh0st and more infection techniques,” Cisco Talos, June 21, 2024, accessed May 9, 2025, https: //blog. talosintelligence. com/sneakychef-sugargh0st-rat/.

264 Smruti S Pattanaik, “China-India rivalry in the Indian Ocean,” last modified March 14, 2024, accessed May 9, 2025, https: //kathmandupost. com/columns/2024/03/14/china-india-rivalry-in-the-indian-ocean.

265 Nicole Fishbein, “Technical Analysis of a Novel IMEEX Framework,” Intezer, October 10, 2024, accessed May 9, 2025, https: //intezer. com/blog/technical-analysis-of-a-novel-imeex-framework/.

266 Chetan Raghuprasad and Ashley Shen, “SneakyChef espionage group targets government agencies with SugarGh0st and more infection techniques,” Cisco Talos, June 21, 2024, accessed May 9, 2025, https: //blog. talosintelligence. com/sneakychef-sugargh0st-rat/.

267 Yin Yeping, “Exclusive: China-Angola ties see great potential as official highlights visible benefits of bilateral cooperation under the Belt and Road Initiative,” The Global Times, September 9, 2024, accessed May 9, 2025, https: //www. globaltimes. cn/page/202409/1319525.shtml.

268 Jamie Harries and Dan Mayer, “LIMINAL PANDA: A Roaming Threat to Telecommunications Companies,” CrowdStrike, last modified November 19, 2024, accessed May 9, 2025, https: //www. crowdstrike. com/en-us/blog/an-analysis-of-lightbasin-telecommunications-attacks.

269 Leon M Chang et al., “Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions,” Trend Micro, November 25, 2024, accessed May 9, 2025, https: //www. trendmicro. com/en_us/research/24/k/earth-estries.html.

270 Gabor Szappanos, “A border-hopping PlugX USB worm takes its act on the road,” Sophos, March 9, 2023, accessed May 9, 2025, https: //news. sophos. com/en-us/2023/03/09/border-hopping-plugx-usb-worm/.

271 Daggerfly: APT Actor Targets Telecoms Company in Africa,” Symantec, April 20, 2023, accessed May 9, 2025, https: //www. security. com/threat-intelligence/apt-attacks-telecoms-africa-mgbot.

272 Tom Hegel, “Cyber Soft Power | China’s Continental Takeover,” SentinelOne, September 21, 2023, accessed May 9, 2025, https: //www. sentinelone. com/labs/cyber-soft-power-chinas-continental-takeover/.

273 “Seeing Through a GLASSBRIDGE: Understanding the Digital Marketing Ecosystem Spreading Pro-PRC Influence Operations,” Google Cloud, November 22, 2024, accessed May 9, 2025, https: //cloud. google. com/blog/topics/threat-intelligence/glassbridge-pro-prc-influence-operations/.

274 Ben Nimmo et al., “Third Quarter - Adversarial Threat Report,” Meta, November 2023, archived December 5, 2024, https: //web. archive. org/web/20241205154209/https: //scontent-lax3-1.xx. fbcdn. net/v/t39.8562-6/406961197_3573768156197610_1503341237955279091_n.pdf?_nc_cat=105&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=W-nmDdyX2MkQ7kNvgFEgogG&_nc_zt=14&_nc_ht=scontent-lax3-1.xx&_nc_gid=ANyIznSrWGrMi2lYwOn632g&oh=00_AYByVhFZiRshbGml_jRUmZgjviVppZdXT0yMMPVpDoVRQQ&oe=6757AA5.

275 James T. Areddy et al., “How China Capitalized on U.S. Indifference in Latin America,” The Wall Street Journal, last modified November 14, 2024, archived May 1, 2025, https: //archive. is/dxssC.

276 Gunthertrigger, ““Operation LongFang” : Attribution and Analysis of a Chinese Cyber Espionage Campaign against Latin American Entities,” Medium, January 24, 2025, accessed May 9, 2025, https: //medium. com/@gunthertrigger/operation-longfang-attribution-and-analysis-of-a-chinese-cyber-espionage-campaign-9716da62b924.

277 Leon M. Chang et al., “Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions,” Trend Micro, November 25, 2024, accessed May 9, 2025, https: //www. trendmicro. com/en_us/research/24/k/earth-estries.html/.

278 Alberto Fittarelli, “Paperwall: Chinese Websites Posing as Local News Outlets Target Global Audiences with Pro-Beijing Content,” The Citizen Lab, February 7, 2024, accessed May 9, 2025, https: //citizenlab. ca/2024/02/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content/.

279 Vanessa Molter, “Seeing Through a GLASSBRIDGE: Understanding the Digital Marketing Ecosystem Spreading Pro-PRC Influence Operations,” Google Cloud, November 22, 2024, accessed May 9, 2025, https: //cloud. google. com/blog/topics/threat-intelligence/glassbridge-pro-prc-influence-operations/.

280 Lior Rochberger and Tom Fakterman, “Squidoor: Suspected Chinese Threat Actor’s Backdoor Targets Global Organizations,” Palo Alto Networks, February 27, 2025, accessed May 9, 2025, https: //unit42. paloaltonetworks. com/advanced-backdoor-squidoor/.

281 Lenart Bermejo et al., “The Espionage Toolkit of Earth Alux: A Closer Look at its Advanced Techniques,“ Trend Micro, March 31, 2025, accessed May 9, 2025, https: //www. trendmicro. com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.html.

282 “Sharp Dragon Expands Towards Africa and The Caribbean,” Check Point Research, May 23, 2024, accessed May 9, 2025, https: //research. checkpoint. com/2024/sharp-dragon-expands-towards-africa-and-the-caribbean/.

283 Alexandre Côté Cyr, “You will always remember this as the day you finally caught FamousSparrow,” ESET, March 26, 2025, accessed May 9, 2025, https: //www. welivesecurity. com/en/eset-research/you-will-always-remember-this-as-the-day-you-finally-caught-famoussparrow/.

284 “Graphican: Flea Uses New Backdoor in Attacks Targeting Foreign Ministries,” Symantec, June 21, 2023, accessed May 9, 2025, https:/ /www. security. com/threat-intelligence/flea-backdoor-microsoft-graph-apt15.

285 US Embassy San Jose, “Costa Rica y EE...,” X, December 17, 2024, accessed May 22, 2025, https: //x. com/usembassysjo/status/1869047401224290614.

286 “Chinese embassy criticizes Costa Rica for 5G company restrictions,” Reuters, last updated October 13, 2023, May 22, 2025, https:/ /www. reuters. com/technology/chinese-embassy-criticizes-costa-rica-5g-company-restrictions-2023-10-13/.

287 I-wei Jennifer Chang, “Guyana Gambit Reveals Taiwan’s Potential Strategic Role in South America,” Global Taiwan Institute, February 24, 2021, accessed May 9, 2025, https: //globaltaiwan. org/2021/02/guyana-gambit-reveals-taiwans-potential-strategic-role-in-south-america/.

288 Robert Evan Ellis. “China expands its presence in Guyana,” Latinoamerica21, September 2, 2023, accessed May 12, 2025, https: //latinoamerica21. com/en/china-expands-its-presence-in-guyana/.

289 Joseph C Chen and Daniel Lunghi, “Earth Krahang Exploits Intergovernmental Trust to Launch Cross-Government Attacks,” Trend Micro, March 18, 2024, accessed May 12, 2025, https: //www. trendmicro. com/en_us/research/24/c/earth-krahang.html.

290 “Guatemala ministry says US embassy's Chinese hack report a years-old case,” Reuters, April 29, 2025, archived April 30, 2025, https: //archive. is/1jVcL.

291 “Guatemala, Taiwan agree to boost diplomatic cooperation, training,” Reuters, last modified September 1, 2022, accessed May 12, 2025, https: //www. reuters. com/world/guatemala-taiwan-agree-boost-diplomatic-cooperation-training-2022-09-01/.

292 “Chinese State-Linked Information Operation Revealed Social Media Account Takeover Potential,” Nisos, July 2023, accessed May 12, 2025, https: //6068438.fs1. hubspotusercontent-na1. net/hubfs/6068438/chinese-info-ops-account-takeover. pdf.

293 “Paraguay kicks out Chinese envoy after he urges country to cut ties with Taiwan,” The Guardian, December 5, 2024, accessed May 12, 2025, https: //www. theguardian. com/world/2024/dec/05/paraguay-chinese-envoy-taiwan.

294 “Joint Statement by the U.S. Embassy in Paraguay and the Ministry of Information Technology and Communication of Paraguay,” U.S. Embassy in Paraguay, November 26, 2024, accessed May 12, 2025, https: //py. usembassy. gov/joint-statement-by-the-u-s-embassy-in-paraguay-and-the-ministry-of-information-technology-and-communication-of-paraguay/.

295 Julieta Pelcastre, “US-Paraguay Strengthen Cybersecurity, Foil China-State Espionage Threat,” Dialogo Americas, December 4, 2024, accessed May 12, 2025, https: //dialogo-americas. com/articles/us-paraguay-strengthen-cybersecurity-foil-china-state-espionage-threat/.

296 Henrietta McNeill and Maualaivao Maima Koro, “Pacific states are setting the terms of diplomatic engagement,” September 11, 2024, accessed May 12, 2025, https: //devpolicy. org/pacific-states-are-setting-the-terms-of-diplomatic-engagement-20240911/.

297 Meg Keen and Alan Tidwell, “Geopolitics in the Pacific Islands: Playing for advantage,” Lowy Institute, January 31, 2024, accessed May 12, 2025, https: //www. lowyinstitute. org/publications/geopolitics-pacific-islands-playing-advantage.

298 Pete McKenzie and Hollie Adams, “Inside the U.S. battle with China over an island paradise deep in the Pacific,” Reuters, April 30, 2025, accessed May 12, 2025, https: //www. reuters. com/investigations/inside-us-battle-with-china-over-an-island-paradise-deep-pacific-2025-04-30/.

299 Christopher K. Colley, "The South Pacific Is the New Frontline in the Rivalry with China," War on the Rocks, March 26, 2025, accessed May 12, 2025, https: //warontherocks. com/2025/03/the-south-pacific-is-the-new-frontline-in-the-rivalry-with-china/.

300 Stephen Dziedzic, “Australia sends expert teams to Fiji as Chinese state-backed hackers attack Pacific Islands Forum,” ABC News, September 11, 2024, accessed May 12, 2025, https: //www. abc. net. au/news/2024-09-12/chinese-state-backed-hackers-attack-pacific-islands-forum/104341412 .

301 Jacob Judah, “A Pacific Island With Ties to Taiwan Was Hacked. Was It Political?,” The New York Times, June 2, 2024, archived June 4, 2024, https://archive. is/QCPGD.

302 Evan Berridge, “Palau Suffers Cyber Attack to Financial Systems,” Atlas News, April 3, 2024, archived April 9, 2025, https: //web. archive. org/web/20240409123650/https: //theatlasnews. co/brief/2024/04/03/palau-suffers-cyber-attack-to-financial-systems/.

303 Albert Zhang and Adam Ziogas, "Russia and China co-ordinate on disinformation in Solomon Islands elections," Australian Strategic Policy Institute, May 2, 2024, accessed May 12, 2025, https: //www. aspistrategist. org. au/russia-and-china-co-ordinate-on-disinformation-in-solomon-islands-elections/.

304 “Advanced Persistent Threat 40 (APT40) Advisory,” SamCERT, February 11, 2025, accessed May 12, 2025, https: //www. samcert. gov. ws/sites/default/files/documents/2025-02/APT40%20-%20SamCERT%20Cyber%20Threat%20Advisory_FINAL_0. pdf.

305 Jacob Judah, “A Pacific Island With Ties to Taiwan Was Hacked. Was It Political?,” The New York Times, June 2, 2024, archived June 4, 2024, https: //archive. is/QCPGD.

306 Albert Zhang and Adam Ziogas, "Russia and China co-ordinate on disinformation in Solomon Islands elections," Australian Strategic Policy Institute, May 2, 2024, accessed May 12, 2025, https: //www. aspistrategist. org. au/russia-and-china-co-ordinate-on-disinformation-in-solomon-islands-elections/.

307 Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," RAND, July 11, 2016, accessed May 8, 2025, https: //www .rand. org/pubs/perspectives/PE198.html.

308 https: //www. china-briefing. com/news/eu-china-relations-after-the-2024-european-elections-a-timeline/.

309 Zhao Junjie, “EU eyes engagement with China amid US pressure,” Global Times, March 31, 2025, accessed May 12, 2025, https: //www. globaltimes. cn/page/202503/1331268.shtml.

310 Plamen Tonchev, “The EU Squeezed Between the US and China,” The Diplomat, March 3, 2025, accessed May 12, 2025, https: //thediplomat. com/2025/03/the-eu-squeezed-between-the-us-and-china/.

311 Vina Nadjibulla, Xiaoting (Maya) Liu, “How Escalating U.S.-China Competition Over Critical Minerals Impacts Canada,” Asia Pacific Foundation of Canada, March 19, 2025, accessed May 12, 2025, https: //www . asiapacific. ca/publication/how-escalating-us-china-competition-over-critical-minerals.

312 Alvin Camba, “A Federal Critical Mineral Processing Initiative: Securing U.S. Mineral Independence from China,” War on the Rocks, April 14, 2025, accessed May 12, 2025, https: //warontherocks . com/2025/04/a-federal-critical-mineral-processing-initiative-securing-u-s-mineral-independence-from-china/.

About Booz Allen

Booz Allen is the advanced technology company delivering outcomes with speed for America's most critical defense, civil, and national security priorities. We build technology solutions using AI, cyber, and other cutting-edge technologies to advance and protect the nation and its citizens. By focusing on outcomes, we enable our people, clients, and their missions to succeed—accelerating the nation to realize our purpose: Empower People to Change the World®.

BoozAllen.com/Cyber

Approved for Public Release. September 2025.