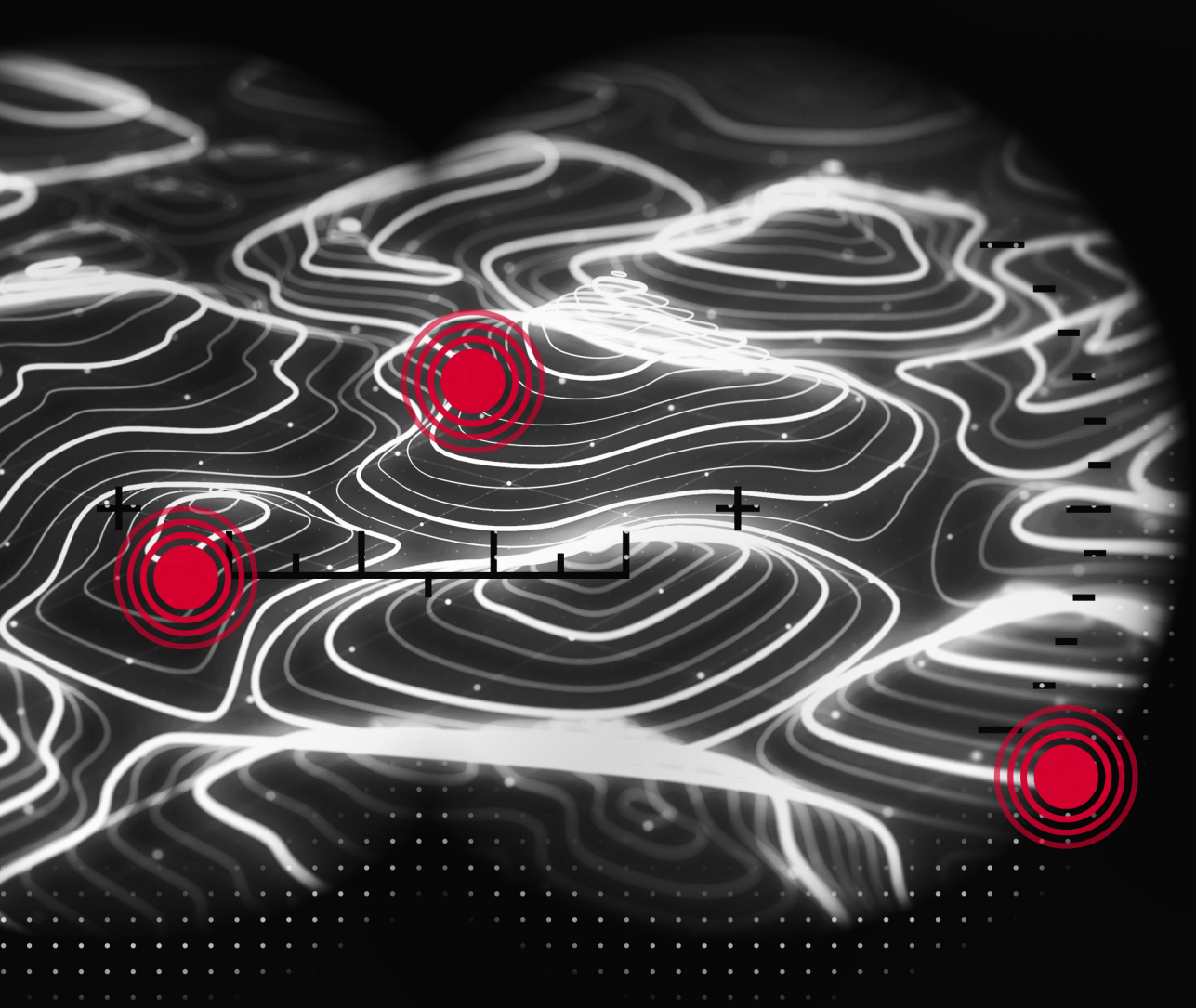

POINT OF VIEW

INTEL 471'S CYBER GEOPOLITICAL INTELLIGENCE

INTEL471

Introduction

Geopolitics and the digital threat environment have converged. Alarming cyber attacks on increasingly digitalized critical infrastructure and fragile supply chains have made the connection between geopolitics and cyber risk stronger than ever. This nexus is being reinforced by armed conflicts that coordinate cyber and kinetic campaigns against critical infrastructure for nation-state goals. Threat actors are exploiting any opportunity to gather valuable strategic information at whatever cost.

In China, government intelligence forces are hiring private information security firms to mount offensive cyber operations across the globe. We're seeing examples of this today. Russia has unleashed destructive disk wiper cyberattacks on Ukrainian critical infrastructure as part of its war efforts. Iran, under the guise of righteous hacktivism, has launched massive influence campaigns to cause chaos in the West.

What the industry is saying

> ***"70% of leaders said that geopolitics influenced their organization's cybersecurity strategy."*** *— World Economic Forum (WEF), Global Cybersecurity Outlook for 2024*

> ***"Today's converged physical and cyber threat landscape has made geopolitical risk assessments a 'must-have, not a nice-to-have' for all sectors."*** *— Forrester analyst, Top Systemic Risks, 2024*

> ***Geopolitical tensions and the finance sector's dependence on digital has increased the probability of a severe systemic cyber incident that undermines macro financial stability.*** *—International Monetary Fund (IMF), Global Financial Stability report, 2024*

At the nexus of political, legal, diplomatic and cyber affairs

Intel 471's Cyber Geopolitical Intelligence offers a full spectrum view of current affairs that directly impact the cyber threat and business landscape in which you operate. We combine open-source intelligence with human intelligence (HUMINT) and other sources for you to accurately assess your digital risks. And we don't stop there. We boost your visibility with tactical knowledge, offering you tailored threat hunting capabilities to harden your security posture.

Types of reports and what they cover

Intel 471's Cyber Geopolitical Intelligence team arms intelligence teams with insights about hostile regions, including China, Iran and Russia. We analyze how states and state-adjacent actors use espionage and information warfare to advance their strategic interests. We also use hypothetical scenarios of real-world conflicts to create stress tests for risk management purposes.

The team provides a regular mix of daily, weekly, fortnightly and quarterly reports.

REPORT	COVERAGE
Spot Reports (daily)	Emerging activity about significant geopolitical events with contextual analysis
Intelligence Bulletins (weekly)	Thematic reports covering country-specific threats, key geopolitical issues and emerging trends
Intelligence Summaries (Bi-weekly)	Insights into significant, trending geopolitical events during a reporting period in China, Iran, Russia, and the "rest of world".
Profile Reports (as needed)	Overview of threat actor or group, including summary of activity, target trends, and TTPs.
Threat Briefs (Quarterly)	Comprehensive reports on a country or regional topic, including in-depth country primer report.

Operationalizing Cyber Geopolitical Intelligence: An analyst's perspective

Intel 471's Cyber Geopolitical Intelligence team has advanced local language capabilities, including Mandarin Chinese, Cantonese (Hong Kong and Taiwan), Russian and Persian, ensuring that context and connotations are not lost in translation. Our reports are customized to the C-suite, security operations, incident response, threat hunting and strategic intelligence teams in mind, depending on the subject matter.

All our reports are available on Intel 471's TITAN platform and structured in line with the General Intelligence Requirement (GIR) framework. TITAN customers with a license for Cyber Geopolitical Intelligence can access all related content.

The following report is an example of our Cyber Geopolitical Intelligence output, and details how we help empower the customer to develop proactive strategies to protect and mitigate against the cyber threats that have become part of the arsenal in geopolitical conflicts.

Sample Intelligence Bulletin

China Escalates Cyberattacks on Critical Infrastructure Amid Geopolitical Conflicts

C-suite leaders can cut through the noise, make informed business decisions and prioritize what's truly important to your organization in just 30 seconds.

Summary

Governments worldwide have called for increased vigilance and tightened security to mitigate Chinese cyber threats targeting critical infrastructure in recent years. This report presents case studies on two Chinese state-linked threats — **APT31** and **Volt Typhoon** — and analyzes their recent cyber operations against vital sectors.

Key findings

- The **APT31** group primarily conducts attacks to exfiltrate valuable information and occasionally targets high-profile organizations to assert China's cyber power.
- The **Volt Typhoon** group prioritizes secrecy and often retargets the same entities over the years to ensure the group maintains access to their information technology (IT) networks with the aim of causing damage at an opportune time such as military clashes.
- Understanding how global geopolitical developments trigger Chinese state-affiliated cyber threat activity can help cybersecurity practitioners anticipate and defend against it.

Strategic intelligence analysts can reap the benefits of concise geopolitical context for a quick grasp of any topic.

Introduction

In April 2024, a key member of the U.S. Indo-Pacific Command cautioned the Chinese Communist Party (CCP) is building capacity to invade Taiwan by 2027 to mark the centennial founding of the People's Liberation Army (PLA). The PLA's modernization also is expected to be complete that year following years of heavy defense investments. Several top U.S. military officers made similar predictions in recent years, although the forecast attack schedule ranges from 2024 to 2027.

In spite of the murky timeline, it is clear China is accelerating its targeting of critical infrastructures abroad, especially in the U.S. Beijing's offensive cyber operations against vital sectors are "both broad and unrelenting" as it pre-positions itself on IT networks for disruptive or destructive cyberattacks.

Why US is key target

Ahead of the U.S. presidential elections in November 2024, U.S. politicians increasingly are arousing anti-China sentiments, calling for enhanced restrictions related to the export of U.S. cutting-edge and emerging technologies, among other things. Sensing a closing window of exploitation, the CCP is trying to seize economic growth under the wire by pilfering American trade secrets before security and trade measures are imposed.

Additionally, China is poised to become the aggressor regarding several flashpoint issues in Asia, including its territorial claims in the South China Sea and reunification with Taiwan. The U.S. has committed to coming to the defense of the Philippines and Taiwan if they were attacked. Crippling U.S. critical infrastructure almost certainly will guarantee widespread panic within the country, serving as a distraction to delay U.S. aid from reaching its allies and partners in the Indo-Pacific.

The following two case studies examine past campaigns of **APT31** and **Volt Typhoon.**

Case study 1: APT31

Security managers can understand the objectives, motivations, activity, targets and TTPs to help security teams prioritize IR, mitigations and recovery.

Target regions, sectors

On March 25, 2024, the U.K. and the U.S. sanctioned Wuhan Xiaoruizhi Science and Technology Co. (Wuhan XRZ) for numerous malicious cyber campaigns that endangered their respective national securities. Seven Chinese nationals were indicted on charges stemming from their involvement in the company. Wuhan XRZ was established in Wuhan, China, in 2010 and is a Ministry of State Security (MSS) front company linked with **APT31**.

Understanding the relationships between cyber perpetrators, governments and front companies also can help cyber security practitioners makes sense of suspicious network activity faster, shortening critical response time.

The **APT31** group is a collection of Chinese intelligence officers, private information security contractors and administrative staff that carry out cyberattacks on behalf of the Hubei State Security Department (HSSD). It primarily targets the U.S. but targets also have been reported in Southeast Asia, Hong Kong, Europe and the U.K.

The cyber threat group targeted the defense industrial base, IT, health care and energy sectors in the U.S. since 2017 and successfully compromised:

- A defense contractor that manufactured flight simulators for the U.S. military.
- A Tennessee-based aerospace and defense contractor.
- An Alabama-based aerospace and defense research corporation.
- A Texas-based energy company.
- A California-based managed service provider (MSP).
- Numerous machine learning (ML) laboratories.
- Multiple health care and medical research facilities.

Operations targeting critical resources

In August 2023, cybersecurity researchers reported **APT31** has targeted industrial organizations in eastern Europe since at least April 2022 to steal

data from air-gapped systems. The threat group used at least 15 distinct implants in each stage of the operations, as well as its signature FourteenHi malware family.

The group's attacks often were timed to coincide with periods of heightened geopolitical tensions between China and the U.S. After the U.S. imposed trade tariffs on China steel imports, China's Ministry of Commerce promised a "major response." A day later, **APT31** started to register infrastructure that impersonated American Steel Co. and the International Steel Trade Forum to use as command-and-control (C2) servers to deploy malware in American Steel's network.

When Hong Kong pro-democracy activists were nominated for the Nobel Peace Prize, **APT31** targeted the Norwegian government and a major Norwegian MSP. The cyber threat group acquired administrator rights that gave it full access to centralized computer systems used by nationwide state administration offices. In 2020, a top U.S. Department of State official called China's broad maritime claims in the South China Sea "completely unlawful," prompting a retaliatory spear-phishing campaign against the U.S. navy and related think tanks.

Case study 2: Volt Typhoon

Target regions, sectors

The **Volt Typhoon** aka **Vanguard Panda, Bronze Silhouette, Dev-0391, UNC3236, Voltzite, Insidious Taurus** group first was discovered in mid-2021 and is a Chinese nation-state group that primarily targets the U.S. — particularly the manufacturing, utility, transportation, construction, maritime, government, IT and education industries. The media brought wider attention to the group's activity in May 2023 when Microsoft revealed its campaign against vital sectors in Guam and across the U.S. Apart from typical espionage, **Volt Typhoon** was pre-positioning itself on critical infrastructure networks with the intent to disrupt or destroy at Beijing's command.

From July 2023 to August 2023, **Voltzite**, an alleged operation technology (OT)-focused unit within **Volt Typhoon,** targeted electric transmission and distribution providers in Africa by compromising industrial control systems (ICSs) and using tactics, techniques and procedures (TTPs) similar to its U.S. campaigns.

Exploiting operational technology security flaws

Since 2021, **Volt Typhoon's** targets and patterns of behavior have strayed from traditional cyber espionage and intelligence gathering operations. The threat group focuses on gaining access to IT networks that will enable lateral movement to OT assets. OT underpins the operations of every critical infrastructure sector, but despite its importance, these systems are notoriously difficult to patch due to stability, accessibility and cost considerations. OT also has a decades-long lifecycle so it often lacks what would be considered as standard security features today such as encryption, which likely was not a priority at the time of build.

Operations targeting critical resources

Common TTPs in **Volt Typhoon's** cyber operations that target critical infrastructure include conducting extensive pre-exploitation reconnaissance and tailoring tactics to the target environment, dedicating ongoing resources to maintain persistence — as long as five years in some cases. The group frequently tests access to domain-joined OT assets by using default OT vendor credentials or compromised credentials in some instances. The group also targets the same entities repeatedly over extended periods to validate and enhance its unauthorized access.

The group uses an array of techniques to ensure its concealment, which include:

- Avoids leaving malware artifacts that would trigger security alerts.
- Deletes logs in a targeted manner.
- Uses living-off-the-land (LOTL) techniques.
- Leverages a botnet of small office-home office (SOHO) routers as intermediate infrastructure to obscure its activity by having C2 traffic emanate from local internet service providers (ISPs) in the target's geographic area.
- Avoids exfiltrating substantial amounts of data. Instead, it typically steals OT-specific data such as supervisory control and data acquisition (SCADA)-related information and geographic information system (GIS) information that could be stored for future disruptive attacks.

Gaining access to these assets gives **Volt Typhoon** the power to:

- Manipulate heating, ventilation and air conditioning systems in secured areas such as server rooms.
- Disrupt critical energy and water controls.
- Access and manipulate camera surveillance systems at critical infrastructure facilities.
- Move laterally to other control systems.

Assessment

We are always looking forward so you can focus on the present. Forecasts the most likely scenarios and how and who they will impact the most.

The two case studies demonstrate how Chinese cyber threat groups with a political agenda can use network access for disruptive effects in the face of geopolitical tensions or military conflicts.

Objectives

The objective of **APT31's** attacks varies but includes stealing diplomatic intelligence and appropriate trade secrets or exfiltrating sensitive information of critical infrastructure personnel. On the other hand, **Volt Typhoon** often exhibits only minimal activity within the compromised environments and stays quietly burrowed deep within target networks for years.

Where **APT31** conducts high-profile proactive and reactive cyberattacks, such as theft or retaliating against anti-CCP entities, respectively, **Volt Typhoon** demonstrates deliberate, long-term cultivation of strategic entryways into foreign countries' most critical sectors that are stored for future use in the event the CCP's interests are threatened.

Targeting

The **APT31** group appears to be more inclined to abruptly pivot targets — from defense agencies to financial organizations — in response to global

geopolitical fluctuations. These targets have included organizations outside critical infrastructure sectors and commonly are highly visible entities in the target country. In comparison, **Volt Typhoon** focuses on breaching entities of various sizes in specific industry verticals, such as utilities, that serve the horizontal market.

The **Volt Typhoon** group targeted small and medium-sized enterprises that provide critical services to large companies and key geographic locations. By compromising vulnerable, smaller third-party vendors with limited cybersecurity capabilities, the threat group can exploit their trusted relationships to gain a foothold in larger partner organizations with robust security practices that otherwise would have been too onerous for **Volt Typhoon** to overcome. This modus operandi will enable **Volt Typhoon** to conduct supply chain attacks without a physical overseas presence.

Tactics, techniques, procedures

The **APT31** group exhibits typical Chinese state-sponsored cyber threat behavior that includes spear-phishing, vulnerability exploitation and the use of custom and off-the-shelf malware and tools. The **Volt Typhoon** group uses hands-on-keyboard, LOTL techniques and botnets to customize and masquerade its presence on breached networks, opting for long-term rather than immediate political gains.

By gauging the CCP's response toward an event, statement or measure, security teams can anticipate incoming waves of Chinese politically and ideologically motivated cyberattacks. Any move perceived to threaten the CCP regime highly likely will trigger a cyber response against foreign entities linked with the issue.

Detection strategy examples

Our custom-built threat hunt packages are tied to exhibited threat behaviors and are therefore critical to detecting APTs and hardening your security posture.

Threat hunting

Proactively hunt for **APT31** behavior and identifiers with custom hunt packs via Intel 471's Hunter platform.

HUNT PACKAGE	LINK
Autorun or ASEP Registry Key Modification	https://hunter.cyborgsecurity.io/research/hunt-package/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c
Scheduled Task Created	https://hunter.cyborgsecurity.io/research/hunt-package/aaa77f56-4a4c-4fdd-a6e3-156e1996d310
File Created in Startup Folder	https://hunter.cyborgsecurity.io/research/hunt-package/8fedb48c-396b-4cd5-9483-69d7fc3eecee
Common Abused Executables Launched Outside of System32	https://hunter.cyborgsecurity.io/research/hunt-package/50641742-9446-4418-a0fa-9ac0fdb9d7dc
Excessive Windows Discovery CommandLine Arguments — Potential Malware Installation	https://hunter.cyborgsecurity.io /research / hunt-package /8bb5819f -06a4 -4e5d -9099 - e43115601999

Proactively hunt for **Volt Typhoon** behavior and identifiers with custom hunt packs via Intel 471's Hunter platform.

HUNT PACKAGE	LINK
Netsh Port Forwarding Command	https://hunter.cyborgsecurity.io/research/hunt-package/0eca36b6-57ef-42b2-bf74-6d0b7dd12aa1
Powershell Encoded Command Execution	https://hunter.cyborgsecurity.io/research/hunt-package/d2d3bbc2-6e57-4043-ab24-988a6a6c88db
Remote Process Instantiation via WMI	https://hunter.cyborgsecurity.io/research/hunt-package/dd0ca1e2-046f-4878-b7f8-32b790420ef2
Dump Active Directory Database with NTDSUtil - Potential Credential Dumping	https://hunter.cyborgsecurity.io/research/hunt-package/98846e7f-c90c-4156-8643-54a613286b66
WMIC Windows Internal Discovery and Enumeration	https://hunter.cyborgsecurity.io/research/hunt-package/bc0fd59c-4217-46a7-a167-764727118567

ABOUT INTEL 471

Intel 471 empowers enterprises, government agencies, and other organizations to win the cybersecurity war using the real-time insights about adversaries, their relationships, threat patterns, and imminent attacks relevant to their businesses. The company's platform collects, interprets, structures, and validates human-led, automation-enhanced intelligence, which fuels our external attack surface and advanced behavioral threat hunting solutions. Customers utilize this operationalized intelligence to drive a proactive response to neutralize threats and mitigate risk. Organizations across the globe leverage Intel 471's world-class intelligence, our trusted practitioner engagement and enablement and globally dispersed ground expertise as their frontline guardian against the ever-evolving landscape of cyber threats to fight the adversary — and win. Learn more at **www.intel471.com.**

Our customers' eyes and ears outside the wire.

INTEL471

1209 N Orange St, Wilmington, DE 19801