

Cyber Affairs Biweekly Report

Chinese Cyber Threats: A Blind Spot in Global Defense Strategies

Major incidents—from Volt Typhoon's targeting of U.S. government agencies, to Middle East energy intrusions, to surveillance of Asia's semiconductor sector—show China's growing cyber presence. As cyber conflict intensifies, organizations face information gaps in the Chinese cyber sphere. Threats, policies, and operations are hard to access and interpret, limiting risk assessment and attacker tracking. Fragmented information, plus language and cultural barriers, complicates compliance and defense. Trusted monitoring and strategic awareness are now essential.

/// Cyber Affairs Biweekly Report: Connecting Global Cyber Strategy

The Cyber Affairs Biweekly Report (aka Biweekly Report) distills TeamT5's Asia-Pacific research, focusing on Chinese policies, regulations, APT activity, and information operations. Each issue covers major events, policy changes, link analysis, and risk assessments—providing a strategic view of threats and integrating APAC intelligence into global planning. Published biweekly, 24 issues annually.

/// Key Highlights

In-depth Analysis of Chinese Cyberspace	APAC Intel Connecting Global Threats	Bridging Chinese Intelligence Gap	Supporting Strategy & Risk Management
Tracks developments & their implications for the global cyber environment.	Integrates regional observations with cross-border activity analysis for assessment.	Contextualized insights from local analysts to identify risks & response priorities.	Covers policy changes, operational trends, risk assessments for allocation & planning.

/// Applicable Roles

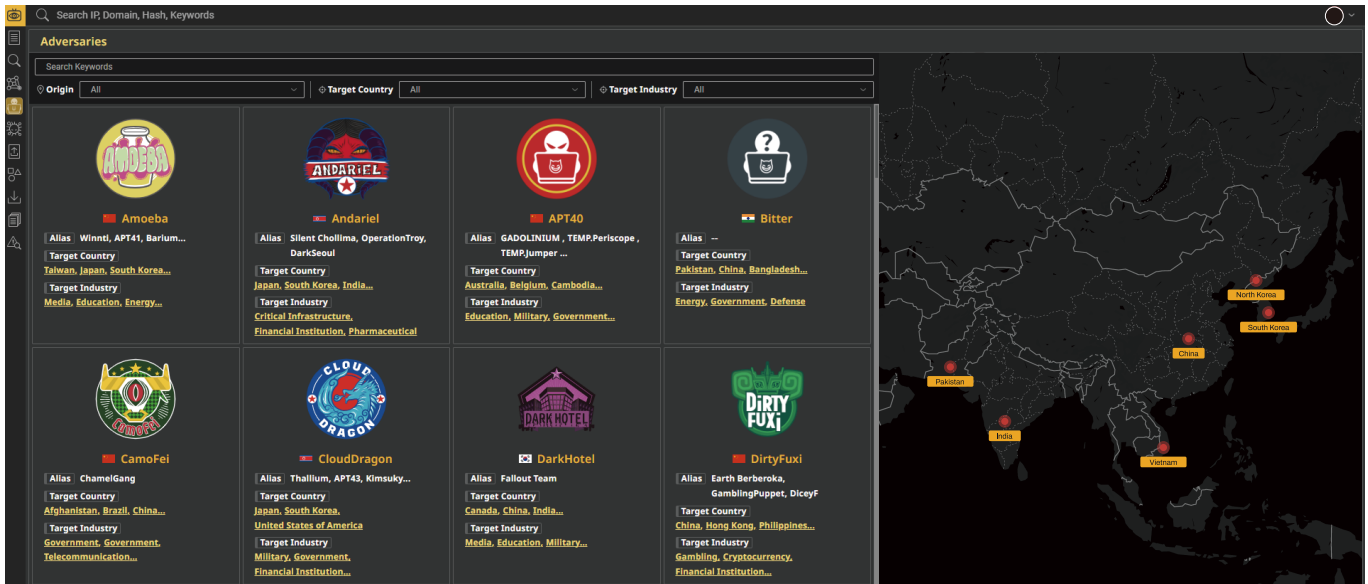
CISOs and Security Strategists	Government and Compliance Officers	Risk and Legal Teams	Security Service Providers
Adjust risk assessments and defense priorities based on policies and threats.	Track policy, regulatory, and information warfare developments in China.	Apply insights to strengthen compliance measures and improve planning efficiency.	Enhance advisory depth and provide higher-value intelligence to clients.

/// From Intelligence to Decisions: Strategic Awareness of the Chinese Cybersphere

The Cyber Affairs Biweekly Report bridges language and information gaps, providing strategic insight into Chinese policy and threat trends. It equips organizations with the intelligence to understand a complex threat environment and maintain strategic advantage in a shifting landscape.

ThreatVision Platform Overview

ThreatVision's diverse intelligence supports various roles and tasks, helping organizations fully grasp the behavioral patterns of adversaries and proactively deploy defensive strategies. It is the optimal solution from strategic planning to frontline defense.



Get Started with ThreatVision

Please contact the TeamT5 sales team to request a 14-day trial account for ThreatVision. For further information, please email sales@teamt5.org. We look forward to helping protect your organization from cyber threats.

About TeamT5

v.202605

Widely trusted by more than 550 customers around the world, including government departments, technology, manufacturing, finance, medical care, military, telecommunications and other industries.

TeamT5 has more than 20 years of experiences in malware and advanced persistent penetration attacks (APT). With language and cultural advantages, we possess specific expertise in cyber espionage in the Asia-Pacific region, and are often invited to present the latest information at world-class cybersecurity conferences, including Black Hat in the United States, Code Blue / AVTokyo in Japan, Troopers in Germany, and Hack In The Box and FIRST. As a world-leading team in the field of threat intelligence research and advanced cybersecurity technology, we have also been interviewed by Bloomberg and CNN in the United States, Sankei Shimbun and Asahi Shimbun in Japan, and ET News in South Korea.