CHINA OSINT:

2026 INTELLIGENCE FORECAST

What We're Seeing — And What's Coming

CLASSIFICATION: OPEN SOURCE
DATE: December 2025
EPCYBER LLC
epcyber.com

EXECUTIVE SUMMARY

Over the last 3 years we're seeing a fundamental shift in how Chinese entities operate, how platforms gradually restrict access, how dual-use technology flows from civilian to military applications, and how AI plays a big role in all of this.

This brief outlines the five points we estimate will define China OSINT work in 2026.

CLASSIFICATION: OPEN SOURCE
DATE: December 2025
EPCYBER LLC
epcyber.com

1. *DUAL-USE TECHNOLOGY — THE CORE CHALLENGE & OPPORTUNITY*

From our monitoring of Chinese policy documents and procurement records, dual-use technology development has accelerated beyond what most Western analysts anticipated.

What we're tracking:

- In 2025 alone, government funding accounted for approximately 400 billion yuan (~$56 billion) of China's projected AI capital expenditure
- Over the past decade, the Chinese government has spent an estimated $900 billion on AI, quantum, and biotech — more than three times U.S. government support for those technologies
- A new multi-billion-yuan national venture capital guidance fund launched specifically for quantum computing, hydrogen energy, and next-generation **information technology**

By 2026, distinguishing between "commercial" and "defense" technology development in China will be functionally impossible. The funding streams, the research institutions, and the personnel all overlap.

CLASSIFICATION: OPEN SOURCE
DATE: December 2025
EPCYBER LLC
epcyber.com

2. *AI-GENERATED CONTENT IS COMPLICATING VERIFICATION*

What we're seeing:
Chinese platforms are flooded with AI-generated content. Deepfakes. Synthetic profiles. Automated posts. State-linked influence operations increasingly use AI to generate personas and narratives.

From our SOCMINT work, distinguishing authentic user content from manufactured content now requires additional verification steps that weren't necessary few years ago.

In 2026, raw social media collection without verification protocols will produce unreliable intelligence. Every SOCMINT workflow needs built-in authenticity checks.

CLASSIFICATION: OPEN SOURCE
DATE: December 2025
EPCYBER LLC
epcyber.com

3. ***PLATFORM ACCESS IS GETTING HARDER***

What we're seeing:
Over the last few years we’re seen that various domestic platform registration requirements are tightening.

From our experience, account creation or even access to content (without registration) and methods or techniques of bypass that worked 18 months ago no longer works today.

By late 2026, anonymous research accounts on major Chinese platforms will be nearly impossible to maintain without sophisticated operational security measures. Investigators without proper access methodology will be locked out entirely.

This is the main reason why we’re making effort to keep our training material up to date with the landscape and the ecosystem * (e.g., ‘China OSINT Advanced’)

CLASSIFICATION: OPEN SOURCE
DATE: December 2025
EPCYBER LLC
epcyber.com

4. ***DATA DELETION IS ACCELERATING***

What we're seeing:
Content that was accessible on Chinese platforms in 2022 is disappearing. Procurement notices. Social media posts. Company filings. Court records.

Government censorship is one factor. But we're also seeing companies proactively scrubbing historical records ahead of regulatory scrutiny. We estimate: The window for historical research is closing.

Investigators who aren't archiving Chinese sources systematically will lose access to critical evidence. What's online today may not be online tomorrow. Therefore, the methodology of working with Chinese data has to adapt.

CLASSIFICATION: OPEN SOURCE
DATE: December 2025
EPCYBER LLC
epcyber.com

5. ***SHELL NETWORKS ARE EVOLVING***

What we're seeing:
Sanctions evasion has moved beyond simple shell companies.

From our investigations, we're tracking entities that don't appear on any restricted list but are operationally controlled by designated parties.

We estimate: Name-based compliance screening will catch fewer violations in 2026. Network analysis — mapping directors, shareholders, addresses, and procurement relationships — becomes mandatory for meaningful due diligence.

CLASSIFICATION: OPEN SOURCE
DATE: December 2025
EPCYBER LLC
epcyber.com