OSINT ON CHINA

SYLLABUS
AUGUST 2025

EPCYBER

Getting Started With OSINT On China

This foundation module goes beyond introductions. It immerses you in the fundamental differences between China's internet ecosystem and the Western web, exposing why many traditional OSINT tools fail and how investigators must rethink their entire approach.

You'll examine censorship mechanisms, real-name identity policies, and layered access restrictions that shape how Chinese users interact online. The module also highlights frequent mistakes Western analysts make and teaches mindset shifts required to succeed in a controlled, closed-off environment.

By the end, you won't just "start" with OSINT on China—you'll rewire how you think, search, and adapt your entire investigation style to fit a highly restrictive digital landscape.

Understanding China’s Linguistic Barriers

China’s internet culture creates a second layer of defense: language. This module equips you to cut through it. You’ll learn to identify hidden meanings in slang, double-layered puns, and coded phrases that often mislead outsiders.

Mis-translations, intentional ambiguity, and regional dialects are turned into investigative puzzles, and you’ll be trained to recognize them. Beyond language skills, you’ll see how communication styles and subcultures influence information flow, and how access barriers can be bypassed without native fluency.

Instead of being lost in translation, you’ll be able to extract meaning, investigate identities, and follow threads that most Western analysts miss completely.

Open Source Intelligence+

Here, OSINT on China goes multi-dimensional. You'll move from surface-level searching to mastering how intelligence disciplines converge in the Chinese context.

GEOINT, IMINT, SOCMINT, and corporate intelligence aren't taught as abstract terms—you'll practice them through case-based tasks and guided exercises. You'll uncover hidden Chinese platforms, use specialized tools and plugins, and test how far you can push OSINT methods in a restricted ecosystem.

Each exercise brings you closer to independence: building the ability to gather, analyze, and fuse data from multiple angles, producing intelligence that goes beyond fragmented glimpses.

Bypassing Restrictions (Access, Limitations)
This module teaches the craft of operating like a local inside China's internet. You'll learn practical ways to bypass access restrictions, obtain real +86 numbers, and create durable accounts without being suspicious on the Chinese platforms.

Rather than relying on high-profile VPNs, you'll adopt field-tested approaches that "exploit" blind spots in China's control mechanisms. Real-world examples and OPSEC lessons ensure you can expand visibility while remaining discreet, maintaining long-term access without detection.

The emphasis is not on "shortcuts" but on developing a professional, sustainable way of moving through China's digital environment undisturbed.

China’s Cyber Threat Ecosystem

Cyber threat intelligence in China isn’t just about hackers—it’s an entire ecosystem. This module maps how threat actors, forums, and underground platforms overlap, evolve, and interact with the surface web.

You’ll learn how to monitor leaks, track dark web chatter, and recognize the structure of China’s unique cybercrime networks. Using avatars and vHUMINT tradecraft, you’ll practice building credible personas that allow deeper engagement.

By the end, you’ll understand China’s cyber threat landscape not as isolated incidents but as a dynamic system of actors, behaviors, and signals that you can read and exploit.

Real-Life Examples, Case Studies, and Practical Exercises

Every lesson in the course is reinforced with reality. This module gathers the techniques you've learned and applies them to authentic scenarios—tracking Chinese actors, extracting data from hidden forums, or reconstructing networks of influence.

Each case study is broken down in detail, showing tools, decisions, and reasoning step by step. You'll then put this into practice with simulated exercises designed to challenge your independence.

The focus is on transfer of skill: by working through progressively complex situations, you build the confidence to carry these methods into real-world investigations without supervision.

Skills You Will Gain from the Advanced OSINT on China Course

Mastering Chinese Context & Culture

- Ability to interpret clusters of Chinese text even without full fluency, using context, and pattern recognition.
- Recognize how meaning shifts depending on region, slang, and subculture.
- Decode the significance of emojis, visual cues, and symbolic references common in Chinese online communities.
- Identify when text is deliberately misleading, sarcastic, or coded to bypass censorship.

Linguistic Intelligence in Investigations

- Spot mistranslations and subtle errors in automated tools that can derail an investigation.
- Understand and apply common idioms, slang, and hacker-specific jargon used across Chinese platforms.
- Recognize “layered meanings” — where a word, emoji, or abbreviation carries double meaning inside underground circles.
- Build a working mental model of communication flows that lets you see how information is exchanged, not just what is said.

Advanced Search & Pivoting Techniques

- Learn to move from one clue to a full investigation: pivoting usernames, IDs, phone numbers, and fragments of text into connected profiles.
- Apply OSINT search techniques across surface, deep, and dark Chinese platforms without relying on standard Western tools.
- Recognize patterns in account creation, metadata, or digital footprints that reveal hidden actors.
- Use one small data point to open up entire networks of related accounts, leaks, or infrastructures.

Cyber Threat and Hacker Community Awareness

- Navigate Chinese hacker slang and community language to spot real actors versus noise.
- Understand the dynamics of underground forums, Telegram/WeChat groups.
- Track how actors disguise themselves through avatars, layered slang, and coded references.
- Recognize behavioral signals of insider threats, cybercriminal groups, or state-backed actors.

Practical Research Mindset

- Develop habits of thinking like a local: how a Chinese user would search, post, or conceal data.
- Learn to balance patience with precision: when to follow deep trails versus pivot quickly.
- Build a low-profile research style with strong OPSEC, blending in and avoiding detection.
- Gain independence: the ability to operate in China’s online environment.

Analytical & Investigative Confidence

- Turn raw data into intelligence products — context-rich, cross-checked, and actionable.
- Apply structured methods to analyze text, images, metadata, and platform behaviors.
- Make judgment calls on credibility, reliability, and hidden bias within Chinese sources.
- Present findings that hold up under scrutiny — whether for corporate security, law enforcement, or national defense.

What This Means for You

By the end of the course, you don’t just “know” how to search China’s internet — you can:

- Extract meaning where others see noise.
- Uncover hidden actors and networks.
- Operate safely and independently in China’s closed-off digital world.
- Produce professional-grade intelligence that rivals automated platforms.