EPCYBER

Advanced OSINT On China

2025 Full Training Syllabus

Includes major February 2025 update of new content, methods, search strategies, techniques.

Download

www.epcyber.com

Course Goals & What You'll Gain

This course was designed to give you real-life, advanced, applicable skills for collecting, analyzing, and producing high quality open-source intelligence from inside the Chinese digital space — a space that remains largely inaccessible to traditional OSINT workflows.

This course focuses on:

Real-life intelligence case studies
Hands-on practice labs, practice what you learned right away
Manual unique techniques that work in the digital field
Verified workflows used by professionals dealing with real Chinese threats and investigations

By the end of the course, you will:

Know how to access, pivot through, and extract intelligence from Chinese platforms and networks despite their restrictions and limitations
Understand the structure and behavior of China's digital ecosystem — from government filters to platform-specific restrictions
Search in Chinese, navigate language challenges, and spot manipulation, bias, and censorship
Map threat actors, identify leaks, and track cyber activity across the clear web, dark web, and deep web
Build and operate sock puppet identities to blend in and interact with restricted closed communities
Use virtual human intelligence (vHUMINT) strategies to engage, gather sensitive data and monitor sources over time

What This Course Includes

5 Fully Updated Full Modules packed with targeted, China-specific OSINT knowledge
50+ of hands-on exercises (Labs) to apply what you learn immediately
Simulation-based practice scenarios that reflect real-world Chinese investigation challenges
Exclusive tactics and methods developed by EPCYBER, not available anywhere else in the West
Search engine lists, keyword libraries, and manual collection techniques
Case studies drawn from live investigations and real access operations
Resource lists to help you continue your research after the course ends
Video Lessons (Live, Pre-Recorded video lessons of hands on investigative sessions)

This course is built for:

Cyber threat intelligence analysts
OSINT analysts
Government and defense personnel
Military, Intelligence personnel
Investigators and researchers focused on China
Red team and security teams dealing with foreign platform activity
Anyone who wants to push beyond the Western limitations and access real information from behind China's digital walls

Module 1: Getting Started With China OSINT

Module Summary

In this module, you'll build a deep understanding of how China's unique digital ecosystem operates — and why traditional OSINT techniques fall short in this space. You'll explore the structure, limitations, and behavioral dynamics of the Chinese internet, as well as the platforms and policies that shape access to information. Through real-world examples, strategic comparisons, and applied context, you'll learn how to re-calibrate your investigative mindset for the Chinese environment. This module lays the foundation for everything that follows — giving you the clarity and orientation needed to operate effectively inside China's online landscape.

Understanding the Basics

- Key differences between China and the West (tools, access, platforms)
- How the Chinese internet is set up and why that matters
- What makes China a difficult target for OSINT investigations
- Common mistakes Western analysts make when starting out

Censorship and Control

- How the Chinese government controls what people can see and post
- What information is blocked or hidden from outsiders
- How platforms like Baidu, WeChat, QQ, and Douyin (TikTok China) work differently
- Why even basic searches don't work the same way in China

Module 1: Getting Started With China OSINT

Access Problems and Limits

- Why some sites are locked if you're outside China
- Real-name rules, ID checks, and phone number requirements
- What happens when you try to use Western tools in Chinese spaces
- How to know if your search method isn't working (how not to fall into rabbit holes in your investigations)

Working Smarter

- What to change in your search approach to find better results
- Where to look first when starting a Chinese OSINT investigation
- Real examples of what works and what doesn't
- How to avoid wasting time and getting stuck

Getting in the Right Mindset

- How to think differently (out of the box) when doing research on China
- How to tell if a tool or platform is worth your time
- What to expect going forward in the course
- Why this foundation is important for everything that comes next

Module 2: Breaking Down Linguistic Challenges

Module Summary

In this module, you'll learn how to deal with the language barrier when doing OSINT in China. You'll see how Chinese is used online, how to search in Chinese even if you don't speak it, and how to spot the difference between different communication forms. You'll also learn how Chinese names work, how to find people, and how to use (and fix) translation tools. This module will help you read faster, search smarter, and avoid common mistakes when working with Chinese content.

Reading and Searching Smarter

- How to read and understand large amounts of Chinese text quickly (context)
- How to search in Chinese correctly, even without knowing the language (strategic approach to searching)
- What to do when automated translation tools fail
- How to quickly tell when your translation is wrong or misleading

Types of Communication in China

- How people communicate in China: text, numbers, symbols, visuals
- The difference between official language and casual or slang messages
- How internet slang, jokes, memes, emojis, and political terms affect your search results
- Why certain words and phrases are hidden or flagged in China

Module 2: Breaking Down Linguistic Challenges

Chinese Names and People Search

- How Chinese names are “built” and why that matters in OSINT
- Tips for finding people in China with limited information
- What strategies work best for name-based investigations

Overcoming Barriers

- Tricks to bypass captchas and access blocked or hard-to-read pages
- Working with Chinese sites and pages that block ability to copy data
- What to do when OCR (text recognition) doesn’t work on Chinese images
- Tools and creative methods to break down language challenges faster

Avoiding Mistakes

- Common errors Western analysts make when dealing with Chinese content
- What to watch out for when using auto-translators or AI tools
- How to check your understanding before taking action on results

Tech Tools for Better Context

- Using AI, plugins, and browser tools to improve language accuracy
- Practical ways to speed up your workflow and reduce confusion (becoming more efficient)

Module 3: Chinese OSINT Disciplines

Module Summary

In this module, you'll dive into the core OSINT disciplines used for deep investigations inside China. You'll learn how to apply different types of intelligence collection — including OSINT, GEOINT, IMINT, SOCMINT, corporate profiling, and people search — specifically for the Chinese environment. Each section is packed with tools, techniques, and real examples and labs that show how to search, bypass restrictions, access hidden data, pivot across sources, and generate valuable intelligence, even when platforms are limited or blocked.

Disciplines Covered:

Open Source Intelligence (OSINT)
Geospatial Intelligence (GEOINT)
Imagery Intelligence (IMINT)
Social Media Intelligence (SOCMINT)
Corporate Intelligence in China
Searching for People in China

Module 3: Chinese OSINT Disciplines

What You Get:

Search engines tailored to Chinese platforms
Reverse search engines for people, images, and for other OSINT disciplines
Tools and plugins that work inside or outside China
Online services that support Chinese intelligence gathering
Step-by-step case studies with full breakdowns
Real-world examples of successful investigations
Exclusive manual methods developed by EPCYBER
Hands-on exercises (Labs) to apply what you learn right away
Resource lists to save time and improve accuracy
Effective Chinese keyword strategies, placement, practices, real world searching
Source development tips to grow your access over time (completely independently!)

You'll learn how to:

Search through restricted or hidden Chinese platforms
Bypass blocks and access sources not visible outside China
Pivot between sources, identities, and tools
Obtain intelligence from corporate, social, or visual data
Discover unknown leads using smart search methods and out of the box approaches
Generate real, actionable intelligence from inside China's ecosystem

*You'll also learn how to apply these methods independently — our strategies are designed to give you long-term capability, so you can replicate everything on your own, even a year after completing the training.

Module 4: Expert Techniques - Bypassing Restricted Access

Module Summary

In this module, you'll learn how to get around the digital barriers that block most people from accessing Chinese platforms and data. From getting a real +86 number to creating accounts and bypassing restrictions without detection, you'll gain hands-on methods for reaching the content and platforms others can't. You'll also learn how to think like a local user, understand the logic behind China's online controls, and apply real-world strategies used by our team to break through access limits. This module is built for professionals who need to go further than search engines — and reach deeper levels of access without raising flags.

Bypassing and Accessing Like a Local

How to get a real +86 Chinese mobile number from outside China
Step-by-step guide to registering Chinese social media and service accounts
How to use platforms that normally block foreign IPs or accounts
Methods that don't rely on VPNs or tools likely to get flagged

Mindset and Strategy

Understanding how the Chinese internet is structured
How Chinese platforms detect and block outsiders — and how to avoid that
Thinking like a local user to reduce friction and raise fewer alerts
Adjusting your approach based on technical challenges

Module 4: Expert Techniques - Bypassing Restricted Access

Manual Techniques and Weak Spots

Spotting the cracks: where China's access controls are weakest
How our team has bypassed real restrictions without paid tools
Field-tested strategies that have worked in live investigations
What methods fail — and how to know when to switch tactics

Real-World Application

A real case example: bypassing state-level restrictions to access blocked content
How to stay low-profile while expanding your access
Building a low-risk footprint for longer-term investigations (OPSEC in Online China)

Note (March 2025):
EPCYBER is actively developing new methods to bypass the GFW, with a focus on overcoming Deep Packet Inspection (DPI) and other advanced filtering mechanisms. These efforts include unique, out-of-the-box tactics designed to bypass geo-based and platform-level restrictions, extending access in even the most controlled environments. Without a VPN, Proxy or typical "solutions" that are commonly known.

Note:
This course is centered on OSINT (Open Source Intelligence) but, where needed, it introduces methods, tools, ideas, and tactics beyond OSINT for a well-rounded approach to intelligence gathering. Occasionally, we'll touch on techniques inspired by penetration testing, used passively only, and as needed to support OSINT objectives, we call that "thinking outside the box".

Module 5: China Cyber Threat Intelligence

Module Summary

In this module, you'll learn how to investigate and monitor cyber threat activity coming from within China. You'll explore how Chinese threat actors operate across the clear web, deep web, and dark web — and how to track their tools, malware, and conversations step-by-step. You'll also learn how to use avatars (sock puppets), engage in virtual human intelligence (vHUMINT), and spot real actors from fakes. This module is designed to help you blend in, gather intelligence, and avoid detection while working in sensitive and unique environments. Practical exercises are included to give you real experience simulating China-focused CTI investigations.

Mapping the Threat Actor Landscape

How to identify and categorize threat actors within China
Understanding motivations: cybercrime, espionage, hacktivism, state-sponsored (APT) ops
Tracking groups through aliases, tools, language, and platform behavior

Multi-Layer Monitoring

Navigating the Chinese dark web, clear web, and deep web spaces
How to locate and monitor underground forums, markets, and restricted networks
Step-by-step guidance to follow threat trails, leaks, and hacking chatter

Module 5: China Cyber Threat Intelligence

Blending In and Engaging Safely

Using avatars and sock puppets to enter and observe CTI spaces
Building profiles that look authentic to Chinese platforms and users
How to gather intelligence without triggering suspicion or bans

vHUMINT for China

Virtual human intelligence techniques tailored for China-specific environments
How to build and maintain local virtual connections and sources
Best practices for ongoing source interaction and info collection

Detection Avoidance and Risk Reduction

How to safely operate in hostile or high-risk digital spaces
Identifying signs you're being "watched" online or flagged
Techniques for reducing exposure and maintaining cover

Investigative Depth and Analysis

Spotting pre-leak signals, zero-day mentions, and threat data references
Differentiating between noise, disinfo, and real threats
How to verify sources, chatter, and tools before acting

We don’t hand out stickers, challenge coins, or t-shirts once you complete the training.

We give you something that actually matters: skills.

Real techniques. Real methods. Real intelligence that you can apply right away at any given moment in your career.

Built for professionals who want results — not souvenirs.

If you’re here to collect knowledge, you’ve come to the right place.

Eva Prokofiev
Founder, CEO, EPCYBER

EPCYBER

EPCYBER is the world's leading provider of China-focused OSINT training — built for professionals who need real access, not surface-level data.

EPCYBER has provided advanced China OSINT training to U.S. and Western intelligence, military, and government and defense teams.

Our methods are built for real-world use — and are trusted by professionals who operate in high-stakes environments where accurate access to Chinese digital intelligence matters.

We teach what actually works when standard OSINT methods fall short.

Every method, tactic, search strategy, insight, and piece of knowledge taught in this training is exclusively developed and authored by EPCYBER LLC, ensuring unmatched originality and proprietary expertise.

EPCYBER