AN INVESTIGATION IN 66 CASES

CHINA IS SPYING ON US

Inside Beijing's Whole-of-Society Espionage Strategy

Case files, organizations, money and techniques, 1985 to 2026

GLOBAL STRATEGY FILES

CHINA IS SPYING ON US

Inside Beijing's Whole-of-Society Espionage Strategy

GLOBAL STRATEGY FILES

globalstrategyfiles.com

Copyright 2026 Global Strategy Files. All rights reserved. This book is a collective work by the contributors of Global Strategy Files. No part of it may be reproduced without written permission, except for brief quotations in reviews and analysis. Facts are current as of November 14, 2026. Persons who have been charged but not convicted are presumed innocent; the facts reported in their cases are allegations made in charging documents or by authorities, and they may be contested. Allegations reported by the press are identified as such.

First edition, November 2026. Published by Global Strategy Files, globalstrategyfiles.com.

Knowledge of the enemy's dispositions can only be obtained from other men.

Sun Tzu, The Art of War, chapter XIII, "The Use of Spies" (translated by Lionel Giles, 1910)

Contents

Section	Title
Introduction	The Naval Enthusiast
Part I	**The Machine**
Chapter 1	A Long History
Chapter 2	The Doctrine
Chapter 3	The Organizations
Chapter 4	The Money
Part II	**The Toolbox**
Chapter 5	Human Techniques
Chapter 6	Front Companies, Money and Export Evasion
Chapter 7	Technical and Cyber Techniques
Part III	**The Cases**
Chapter 8	United States
Chapter 9	The AI Chip Pipeline
Chapter 10	Europe
Chapter 11	Canada and Australia
Chapter 12	Taiwan: The Front Line
Part IV	**The Digital Front**
Chapter 13	Salt Typhoon and Volt Typhoon
Part V	**The Response**
Chapter 14	The West Strikes Back, and Beijing's Mirror
Chapter 15	Three Scenarios to 2030
Part VI	**The Deeper Stakes**
Chapter 16	The Shopping List: What Beijing Wants and Why

Section	Title
Chapter 17	The Corporate Front: How Companies Lose Their Crown Jewels
Chapter 18	What Espionage Is Worth: Losses for the West, Gains for China
Chapter 19	The Defenders: Is Western Counterintelligence Built for This?
Chapter 20	The Campus Question: Research Security Without Suspicion by Ancestry
Chapter 21	The Information Front: When Collection Meets Persuasion
Chapter 22	Machines That Spy: Artificial Intelligence and the Next Phase
Chapter 23	Three Espionage Powers: China Compared with the Soviet Union and Russia
Part VII	**The Wider Battlefield**
Chapter 24	The Hacker Economy: Contractors, Bounties and the Market for Intrusion
Chapter 25	The Physical Layer: Cranes, Cables, Antennas and Ground Stations
Chapter 26	Data by Design: When Commerce Becomes a Collection Channel
Chapter 27	The Asian Allies: Japan and South Korea Rebuild Their Defenses
Chapter 28	The Long Arm and the Locked Door: Law as an Instrument Against Exiles and Foreigners
Chapter 29	The Southern Flank: The Philippines, Scam Hubs and an 85-Year-Old Law
Conclusion	Living With a Sensor State
Annexes	
Annex A	The GSF Database of Public Cases: Method and Summary
Annex B	Timeline of Major Cases, 1985 to 2026
Annex C	Glossary
Annex D	Budget Estimate: Data and Assumptions
Annex E	Practical Guide: Detecting and Resisting a Recruitment Attempt

Section	Title
Annex F	Sources and Bibliography
Annex G	Case Files
Annex H	Organizational Profiles
Annex I	Countermeasures and Legal Responses, 2018 to 2026

List of Figures, Charts and Tables

Figures

- Figure 1.1. Public cases of Chinese espionage in the West, by period
- Figure 3.1. The Chinese espionage apparatus

Charts

- Chapter 8. Outcomes of the public cases in the GSF database
- Chapter 9. Alleged values of AI chip smuggling to China
- Chapter 10. European cases by country
- Chapter 12. Espionage prosecutions in Taiwan and military pressure
- Chapter 14. The shift in the nature of public cases, before and after 2020
- Chapter 16. Main targets of the cases in the GSF database

Tables and boxes

- Table 2.1. The legal framework of Chinese intelligence
- Table 4.1. Selected items of the 2026 central budget
- Table 4.2. GSF estimate of China's intelligence spending (illustrative)
- Table 4.3. Intelligence efforts compared (orders of magnitude)
- Table 5.1. Motivations in Chinese espionage cases
- Box 5.1. Five warning signs of a recruitment attempt
- Table 6.1. Techniques used to smuggle restricted AI chips to China
- Table 7.1. Major breaches of personal data attributed to China
- Table 7.2. The Chinese espionage toolbox
- Table 13.1. The Typhoon campaigns, key dates
- Table 15.1. The three scenarios compared
- Table 19.1. Legal tools against espionage and foreign interference

- Table 23.1. Three models of espionage power
- Table 25.1. Infrastructure cases: evidence and function
- Table 27.1. Japan and South Korea: from legal gaps to new frameworks
- Table I.1. Selected countermeasures and legal responses
- Table C.1. The main findings of this book
- Table A.1. Summary of the database
- Table A.2. Outcomes by family

Abbreviations

Abbreviation	Meaning
APT	Advanced persistent threat (a state-backed hacking group)
ASIO	Australian Security Intelligence Organisation
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
CMC	Central Military Commission
DGSE	Direction générale de la sécurité extérieure (France)
FBI	Federal Bureau of Investigation
MPS	Ministry of Public Security
MSS	Ministry of State Security
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
PLA	People's Liberation Army
SHAPE	Supreme Headquarters Allied Powers Europe
UFWD	United Front Work Department

Introduction: The Naval Enthusiast

In 2022, a young machinist's mate on the amphibious assault ship USS Essex received a message on social media from a man who presented himself as a naval enthusiast working for a Chinese state shipbuilding company. The man wanted to know where American warships were docked and offered 500 dollars to find out. The sailor, Jinchao Wei, told a fellow sailor that this was obviously espionage. He went ahead anyway. Over eighteen months, according to the evidence at his trial, he sent his contact photographs and videos of his ship, information about its defensive weapons, the locations of other vessels and dozens of technical and operating manuals taken from restricted Navy computer systems. He was paid a little more than 12,000 dollars. Arrested in August 2023 as he reported for duty at Naval Base San Diego, he was convicted of espionage by a federal jury in August 2025 and sentenced in January 2026 to 200 months in prison.

Nothing about the case was spectacular. The recruiter approached his target online, used a plausible cover story and small sums of money, and asked for information that a junior sailor could reach from his workstation. That is precisely why the case matters. It shows a method that costs little, can be repeated thousands of times and needs only one success among many refusals. And it captures something larger: the sense that Chinese espionage has moved from the margins of national security into the everyday life of Western institutions, their warships and laboratories, their parliaments and military headquarters, and the phones of the people who work in them.

The rest of 2026 made the point. In July 2026, Belgian police arrested a Canadian intern working in the information technology department of NATO's military headquarters in Mons, on suspicion of

spying for a third country that security sources identified as China. In September, Britain's domestic security service, MI5, published its first ever public espionage alert, warning that more than one hundred academics linked to British universities had worked on projects funded by an institute it said existed to improve the technical capabilities of China's civilian intelligence service. In October, an American cybersecurity firm revealed that a Chinese state hacking group had spent three years building a hidden network to break into telecommunications providers, defense contractors and utilities. And throughout the year, American prosecutors charged one network after another with smuggling restricted NVIDIA processors to China through Malaysia, Singapore and Thailand, in one case allegedly worth about 2.5 billion dollars.

This book is about the strategy behind these cases.

An industrial-scale enterprise

Espionage is as old as the state, and every major power practices it. The United States, Britain and France run intelligence services that recruit foreign officials and intercept foreign communications. China itself accuses the American National Security Agency of hacking its infrastructure. Any honest account of Chinese espionage has to start from that fact.

What sets China apart is not that it spies, but how much, on what, and with whom. Britain's parliamentary intelligence committee concluded in 2023 that China's state intelligence apparatus is almost certainly the largest in the world, with hundreds of thousands of civilian intelligence officers. The same committee described a "whole-of-state" approach in which state-owned and private companies, academic and cultural institutions and ordinary citizens can be co-opted, willingly or not, into espionage and interference. Former FBI director Christopher Wray said in 2020 that his bureau was opening a new China-related counterintelligence case about every ten hours, and that nearly half of its roughly 5,000 active counterintelligence cases involved China. In 2023, MI5's director general

said that more than 20,000 people in the United Kingdom had been approached online by Chinese agents.

These numbers describe an enterprise of a different kind from the espionage of the Cold War. The Soviet Union ran a small number of highly trained officers who recruited a small number of carefully chosen sources. China runs professional officers too, but it also draws on a vast population of what American officials call non-traditional collectors: students, researchers, engineers, businessmen, community leaders and contractors, each of whom may gather a small piece of a much larger picture.

The argument of this book

Our central claim is simple: **China did not invent a new kind of espionage; it industrialized the old one.** It has turned espionage from the work of a specialized service into a function of the whole state and, potentially, of the whole society. Laws oblige citizens and organizations to cooperate with intelligence work. Talent programs, research funding, investment and trade create channels through which knowledge flows. Cyber operations collect at a scale no human network could match. And the result is assembled at the center, in the service of three goals: catching up with and overtaking the West in technology, protecting the Communist Party's hold on power at home and abroad, and preparing for a possible conflict over Taiwan.

Three features of this strategy recur throughout the book.

- **It is broad.** It targets military secrets, but also commercial technology, academic research, political decision-making and the private lives of dissidents. A wind tunnel design, a battery formula, a parliamentary negotiation and the address of an exiled activist are all worth collecting.
- **It is patient.** Cases often span years or decades. A French intelligence officer's relationship with an interpreter in Beijing in the late 1990s led to a treason conviction in 2020. A German agent

was, according to prosecutors, working for Chinese intelligence from 2002 until his arrest in 2024. Hacking groups have stayed inside networks for years before being detected.

- **It blurs lines.** Between civilian and military, between commerce and espionage, between influence and intelligence, between a state agency and a private company. This blurring is not an accident. It is the design.

Why the West keeps being surprised

If the strategy is so large, why does each new case come as a shock? Part of the answer lies in the openness of Western societies. Universities welcome foreign students and researchers. Companies seek Chinese customers and investors. Parliaments hire staff without the vetting applied to intelligence officers. Networks are built on equipment that is rarely patched. Openness is a strength, and it is also an exposure.

Another part of the answer lies in Western ambivalence. For three decades, Western governments saw China first as a market and a partner. Warnings from security services were often heard as obstacles to trade. In Britain, a major espionage prosecution collapsed in 2025 because the government would not certify that China met the legal definition of a threat to national security. In the United States, an aggressive program launched in 2018 to fight Chinese economic espionage, the China Initiative, was abandoned in 2022 after it produced few espionage convictions and many accusations of profiling Chinese Americans. Both failures show how hard it is to respond to a threat that is real without damaging the open society it targets.

What is new in this book

This book brings together, in one place and as of November 2026, the evidence that is usually scattered across court filings, intelligence reports, think tank studies and news reports. It offers four contributions.

First, **real cases across the Western world**. The book examines cases in the United States, Germany, Britain, France, Belgium, Greece, the Netherlands, Norway, Canada, Australia and Taiwan, from the CIA translator Larry Wu-tai Chin in 1985 to the smuggling of AI chips in 2026.

Second, **the techniques**. Part II sets out how China collects: the online approach, the hotel room, the honey trap, the insider, the front company, the research grant, the transit country, the router, the relay network.

Third, **the organizations and the money**. Part I describes the agencies that run Chinese espionage, from the Ministry of State Security to the military forces created in 2024, and attempts what is rarely done: an estimate of the resources China devotes to intelligence, despite the secrecy of the budget.

Fourth, **an original database**. Global Strategy Files has compiled a database of public cases of Chinese espionage in the West, coded by year, country, target, technique, suspected organization and judicial outcome. In its first version it holds seventy cases. Its figures appear throughout the book and its method is set out in Annex A.

A note on evidence

Espionage is secret by definition, and much of what is written about it rests on claims that cannot be checked. This book follows three rules.

1. **We distinguish what is proven from what is alleged.** A conviction, a guilty plea, an indictment, an arrest, an intelligence assessment and a press report are not the same thing, and we say which one we are relying on. People who have been charged but not convicted are presumed innocent.
2. **We report failures as well as successes.** Cases that collapsed, prosecutions that were dropped and accusations that proved unfounded are part of the story, because they show the limits of the evidence and the costs of overreaction.

3. **We give Beijing's view.** China denies almost every accusation and accuses the United States of the same conduct. Chapter 14 examines those counter-accusations seriously, without adopting them.

Most of the statistics available on Chinese espionage come from Western and Taiwanese security services, which have an interest in highlighting the threat. Where a figure is contested, such as the often-cited estimate that intellectual property theft costs the United States between 225 and 600 billion dollars a year, we explain why.

How the book is organized

Part I, The Machine, explains how Chinese espionage is built: its history (Chapter 1), its doctrine and laws (Chapter 2), its organizations (Chapter 3) and its money (Chapter 4).

Part II, The Toolbox, sets out the techniques: human methods (Chapter 5), front companies, research funding and the evasion of export controls (Chapter 6), and technical and cyber methods (Chapter 7).

Part III, The Cases, examines real cases: in the United States (Chapter 8), in the smuggling of AI chips (Chapter 9), in Europe (Chapter 10), in Canada and Australia (Chapter 11) and in Taiwan (Chapter 12).

Part IV, The Digital Front, is devoted to the two great Chinese cyber campaigns, Salt Typhoon and Volt Typhoon (Chapter 13).

Part V, The Response, weighs the Western response and Beijing's counter-narrative (Chapter 14) and sets out three scenarios to 2030 (Chapter 15).

Part VI, The Deeper Stakes, steps back from the cases. It compares the targets of Chinese espionage with Beijing's industrial plans (Chapter 16), follows companies from the inside as they lose their crown jewels (Chapter 17), asks what espionage is really worth to the West and to China (Chapter 18), examines whether Western

counterintelligence is built for the threat (Chapter 19), weighs research security against suspicion by ancestry (Chapter 20), connects espionage to China's information operations (Chapter 21), assesses how artificial intelligence changes the contest (Chapter 22) and compares China with the Soviet Union and Russia as espionage powers (Chapter 23).

Part VII, The Wider Battlefield, widens the lens beyond spies and agents. It describes the market of contractors behind Chinese hacking (Chapter 24), the physical infrastructure that can serve as sensor or lever, from port cranes to seabed cables and ground stations (Chapter 25), the commercial channels through which data flow to companies subject to Chinese law (Chapter 26), the struggle of Japan and South Korea to close their legal gaps (Chapter 27), the use of law itself against exiles abroad and foreigners in China (Chapter 28) and the Philippines, where military reconnaissance, organized crime and an outdated law meet (Chapter 29).

The **Conclusion** asks what it means to live alongside a state that treats its whole society as a potential sensor. The **Annexes** present the database, a timeline, a glossary, the budget estimate, a practical guide to resisting recruitment and the sources, followed by a file on every case in the database (Annex G), profiles of the Chinese organizations involved (Annex H) and a timeline of countermeasures and legal responses (Annex I).

The story of Chinese espionage is often told as a series of scandals. This book tells it as a strategy: coherent, patient, imperfect and, for the West, still poorly understood.

PART I: THE MACHINE

Before we can understand a single case, we need to understand the machine that produces them: where it comes from, what it believes, who runs it and what it costs. Part I takes the machine apart.

Chapter 1. A Long History

The idea that Chinese espionage is a recent phenomenon, born with China's economic rise, does not survive a look at the record. Beijing has been running agents inside Western institutions for as long as the People's Republic has existed. What has changed is not the existence of Chinese espionage but its scale, its targets and its methods. This chapter follows that evolution through the cases that defined each period, from a single agent inside the CIA to the thousands of collectors and hackers of today.

1.1 The first great case: thirty years inside the CIA

Larry Wu-tai Chin was born in Beijing in 1922. He worked for American military offices in China in the 1940s and later joined the Foreign Broadcast Information Service, a branch of the CIA that translated and analyzed foreign media. For three decades he was a trusted translator with access to sensitive material. He was also, according to the case brought against him, an agent of Chinese intelligence from before he joined the agency until his retirement in 1981.

Chin was arrested in November 1985, after information from a Chinese defector pointed American counterintelligence toward him. He was convicted in February 1986 and died in his cell before he could be sentenced. His case set a pattern that would recur for decades: a long-term agent, recruited early, often of Chinese origin, placed not in the operational heart of an intelligence service but in a position that gave steady access to documents. It also revealed a lesson that American counterintelligence would relearn several times: Chinese services are patient. They are willing to wait years, even decades, for a source to mature.

1.2 The 1990s and 2000s: nuclear secrets and naval propulsion

In the 1990s, American attention turned to nuclear weapons. A congressional investigation concluded in 1999 that China had obtained design information on advanced American warheads. The search for a culprit led to Wen Ho Lee, a Taiwanese-born physicist at the Los Alamos National Laboratory. Lee was arrested in 1999, charged with 59 counts and held in solitary confinement for months. The case then collapsed. In 2000 he pleaded guilty to a single count of mishandling information, and the federal judge apologized to him from the bench for the way he had been treated.

The Wen Ho Lee affair became a reference point for two opposite lessons. For some, it showed the reality of the threat: sensitive information had been handled carelessly at the heart of the American nuclear complex. For others, it showed the danger of suspicion based on ethnicity, and the damage that a failed prosecution can do to individuals and to the trust of entire communities. Both lessons remain alive today, and both are needed to understand the debate around the China Initiative two decades later.

The 2000s brought clearer cases. In 2005, the FBI arrested Chi Mak, an engineer at a Californian defense contractor working on naval propulsion systems, after his brother was caught preparing to fly to Hong Kong with encrypted discs containing technical documents. Mak, who had lived in the United States for decades, was convicted in 2007 and sentenced to more than two decades in prison. The case showed a family network, a long period of quiet collection and a focus on the technologies that would allow China's navy to become quieter and harder to detect.

The same years exposed the vulnerability of American counterintelligence itself. Katrina Leung, a Los Angeles businesswoman, had served for some twenty years as a highly paid FBI informant on Chinese affairs while maintaining intimate relationships with the agents who handled her. In 2003 she was charged with taking classi-

fied documents from one of them. The suspicion that she had worked for Beijing all along shook the bureau. The case ended in a guilty plea to minor charges, but it remains a study in how a double agent can blind a service from within.

1.3 France's lesson: the station chief and the interpreter

Europe was not spared. The most damaging case known to the public is French. In 1997, the French foreign intelligence service, the DGSE, posted an officer known in court as Henri M. to its station in Beijing under diplomatic cover. Within months he was recalled, after the service discovered that he had begun a relationship with the Chinese interpreter of the French ambassador. He later retired, returned to China and married her.

Two decades later, in December 2017, Henri M. and a former colleague, Pierre-Marie H., a former civilian employee of the defense ministry, were arrested on suspicion of having passed secrets to China. The case had been detected by the DGSE itself. The trial was held behind closed doors in 2020. Both men were convicted of treason; Henri M. received eight years in prison and Pierre-Marie H. twelve. The wife of Pierre-Marie H. was also convicted. The affair had already forced the DGSE to recall several officers from China.

The French case illustrates a technique as old as espionage itself, the honey trap, and a time frame that only a patient service can afford: the first contact in Beijing in the late 1990s, the conviction in Paris in 2020. It also shows that Chinese services were able to penetrate one of the most secretive intelligence agencies in Europe.

1.4 The age of the recruited student and the online approach

In the 2000s and 2010s, Chinese services refined a method that would become central: recruiting Westerners while they were young, abroad or professionally vulnerable.

The case of Glenn Duffie Shriver is the classic example. An American student in Shanghai, Shriver answered an advertisement offering payment for a paper on relations between the United States and China. The contact led to meetings with Chinese intelligence officers, payments and a request: apply for jobs in the American government. Shriver applied to the State Department and to the CIA's clandestine service. He was arrested in 2010 and sentenced to four years in prison. The FBI later turned his story into a training film for students going abroad.

The next step was the internet. In 2017, Kevin Mallory, a former CIA officer in financial difficulty, was contacted through a professional networking site by a person posing as a recruiter for a think tank. The contact led him to Chinese intelligence officers, to whom he sold classified documents. He was sentenced to twenty years in prison in 2019. The same year, Jerry Chun Shing Lee, another former CIA officer, was sentenced to nineteen years for conspiring to spy for China. Investigators had long suspected a link between the collapse of the CIA's network of sources in China in the early 2010s and a mole, though the full story has never been made public.

These cases mark a shift. Chinese services were no longer waiting for sources to come to them or relying only on people of Chinese origin. They were actively hunting for Westerners with access and weaknesses, using the open tools of the digital age.

1.5 The cyber revolution

At the same time, a new form of collection was transforming the scale of Chinese espionage. In 2013, an American cybersecurity firm published a detailed report attributing years of intrusions into Western companies to a unit of the People's Liberation Army based in Shanghai, Unit 61398. In 2014, the United States indicted five officers of that unit for hacking American companies in the nuclear, steel and solar industries. It was the first time a government had charged officials of another state with cyber espionage for commercial advantage.

The following year brought one of the most damaging intrusions in American history. Hackers attributed to China stole the records of about 21.5 million current and former federal employees and applicants from the Office of Personnel Management. Those files contained the most intimate details of the lives of people with access to secrets: finances, relationships, health, foreign contacts. For an intelligence service seeking people to recruit, they were a catalog.

In September 2015, President Obama and President Xi Jinping agreed that neither government would conduct or knowingly support the cyber-enabled theft of intellectual property for commercial advantage. Some observers noted a temporary decline in certain Chinese intrusions after the agreement. But the deal did not cover espionage against governments, and the broader campaign continued. Chapter 13 shows how it evolved into the operations known as Salt Typhoon and Volt Typhoon.

1.6 The first extradition and a new American offensive

In April 2018, Belgian authorities arrested Xu Yanjun, a deputy division director in China's Ministry of State Security, who had traveled to Brussels to meet an engineer of GE Aviation. The engineer had been cooperating with the FBI. Xu was extradited to the United States, the first Chinese intelligence officer ever brought to trial there. Prosecutors showed that he had targeted employees of several aviation companies, invited them to China for presentations and, with colleagues, copied their computers in their hotel rooms while they were taken to dinner. He was sentenced to twenty years in prison in 2022.

The Xu case opened a window into the operational methods of the MSS and its ties to China's aviation industry. It was also the beginning of a more aggressive American posture. In November 2018, the Justice Department launched the China Initiative, a program to prioritize cases involving Chinese economic espionage. The program produced some significant convictions but became better known for prosecutions of academics for failing to disclose Chinese ties,

several of which collapsed. It was ended in February 2022. Its record is examined in Chapters 6 and 14.

1.7 From a few professionals to thousands of collectors

By the end of the 2010s, the pattern had changed in three ways.

- **Volume.** In 2020, the FBI said that economic espionage cases with a link to China had increased by about 1,300 percent over a decade. In Taiwan, the number of people prosecuted for spying for China rose from 16 in 2021 to 64 in 2024.
- **Diversity of collectors.** Alongside career officers, cases now involved students, researchers, engineers, businessmen, community leaders, parliamentary aides, interns and soldiers.
- **Diversity of targets.** Beyond military secrets, collection reached commercial technologies, university research, political decisions and the diaspora.

The Global Strategy Files database captures this evolution in the cases that have become public.

Figure 1.1. Public cases of Chinese espionage in the West, by period (GSF database, first version, 68 entries)

Period	Number of cases
Before 2010	5
2010 to 2019	12
2020 to 2024	28
2025 and 2026	23

These figures must be read with care. They reflect what has become public, not the full extent of Chinese activity, and the database is more complete for recent years than for earlier decades. A rise in cases can also reflect greater vigilance by Western services. But the trend is consistent with what every Western security service says: Chinese espionage has intensified, and the West has started to look for it.

1.8 What history teaches

Four lessons emerge from forty years of cases.

1. **Patience is a Chinese advantage.** Sources are cultivated over years and sometimes decades. A Western counterintelligence culture built around short political cycles struggles to match that time frame.
2. **The method adapts to the medium.** From personal relationships to newspaper advertisements, from networking sites to hacked databases, Chinese services have used each new tool as it appeared.
3. **Failure is costly on both sides.** Failed prosecutions, from Wen Ho Lee to the China Initiative, have damaged innocent people and weakened the credibility of real warnings.
4. **The scale has changed the nature of the problem.** When collectors number in the thousands, the response cannot rely only on catching individual spies. It requires understanding the system that sends them.

That system is the subject of the next three chapters: the doctrine that drives it, the organizations that run it and the money that funds it.

Notes to Chapter 1

- Federal court records and contemporary reporting on the cases of Larry Wu-tai Chin (1985 to 1986), Wen Ho Lee (1999 to 2000), Katrina Leung (2003 to 2005), Chi Mak (2005 to 2008), Glenn Duffie Shriver (2010), Kevin Mallory (2017 to 2019) and Jerry Chun Shing Lee (2018 to 2019).
- Reporting by AFP, Reuters, Le Monde and France Info on the trial of two former DGSE officers (July 2020).
- US Department of Justice, sentencing of Yanjun Xu (November 16, 2022).

- FBI, speech of Director Christopher Wray at the Hudson Institute (July 7, 2020).
- Taiwan National Security Bureau, Analysis on the Infiltration Tactics Concerning China's Espionage Cases (January 2025).
- Global Strategy Files database of public cases, first version (November 2026).

End of the free excerpt

The complete book, with twenty-nine chapters in seven parts, a conclusion, nine annexes, a file on each of the 66 cases in the database and profiles of the Chinese organizations involved, is available as a PDF at globalstrategyfiles.com.

CHINA IS SPYING ON US

Inside Beijing's Whole-of-Society Espionage Strategy

A sailor recruited online by a man posing as a naval enthusiast. An assistant inside the European Parliament. A satellite dish in a holiday rental in southwestern France. Servers worth billions shipped in dummy boxes. Hackers inside the networks that carry the West's phone calls.

Built on a new database of 66 public cases from 1985 to 2026, this book shows how Beijing turned espionage into a function of the whole state: the laws that oblige cooperation, the organizations that run the operations, the money behind them and the techniques, from online recruitment to chip smuggling and the Typhoon hacking campaigns, and on to contract hackers, port cranes, seabed cables and commercial data.

The findings are new and uncomfortable. Western courts convict classic spies but struggle with the fastest-growing forms of collection. Cyber intruders almost never face trial. And the most valuable technology now leaves through trade, not theft.

66
public cases, each with its own file

15 to 45
billion dollars a year of state intelligence spending (GSF estimate)

8 of 15
cyber cases with no prosecution

3
scenarios for Chinese espionage to 2030

ABOUT THE AUTHOR

Dr. Driss Effina holds a PhD in Political Economy and has extensive international teaching experience across several universities. With nearly 100 academic publications, his research focuses on global political economy, regional conflicts and international relations. He closely follows the evolution of global policies and conflicts, offering analyses and anticipations of major geopolitical events. He leads Global Strategy Files, an independent research platform.

GLOBAL STRATEGY FILES
GLOBALSTRATEGYFILES.COM