

# AMERICAN LOSER

WHEN DOMINANCE FALTERS:  
**AMERICA**'S ACCUSATIONS  
OF **TECHNOLOGY THEFT** &  
THE NARRATIVE OF  
**COMPETITIVE INSECURITY**

ERIC YEW KEE WONG <sup>+Ai</sup> © (2028)

## AUTHOR'S BACKGROUND

**Yew Kee WONG (Eric)** is a former Professor, Associate Vice-President, & Registrar at Hong Kong Chu Hai College. He has previously served as a Professor at BASIS. He holds a BSc (Hons) degree in Computing Systems & a PhD in Ai from Nottingham Trent University (NTU), UK. When he was 15 & 19, he was the youngest undergraduate & PhD student admitted to NTU. Between 2001 & 2016, he was the Senior Programme Director at The University of Hong Kong (HKU-SPACE). His research interests include Ai, Quantum Computing, Web3 Technology, & Big Data Analytics. Over the last 30 years, he has been granted & received over USD\$10 million in research funding from Governments, Private Foundations & Institutions (from Europe, Africa & Asia).

Prof. WONG (Eric) has served on more than 3,000 top-tier International Conference Chairs, Scientific/Publicity Chairs & Program/Technical Committees. Since 2005, he has actively participated in 52 International Journals as Editor-in-Chief, Associate Editor, & Member of the Journal Editorial Board Committee. He is currently a Fellow, Professional & Individual member of 12 Internationally renowned Professional Organizations (IEEE, ACM, AAAI, IIBA, ISACA, AIP, BCS, IOA, ACL, CAIAC, AAIA & ICAIL).

During his career, he has held the titles of Honorary Professor, Distinguished Professor, Adjunct Professor, Visiting Professor & Honorary Research Fellow at 15 different universities & institutions. From 1996 to present, he has published more than 250 e-book titles (e-Print [PDF], self-authored<sup>+Ai</sup>) and over 190 peer-reviewed articles & research papers in top-tier academic journals, conference proceedings, and online R&D outlets. Many of his research papers have appeared in world-renowned journals such as Scientific Reports, Springer Nature & IEEE. Additionally, he has served as a UNICEF (UN) Volunteer since 2018. He has supervised/co-supervised over 100 PhD/Master students.



**Professor Dr. Yew Kee WONG Eric**

Website: <https://ericylewkeewong.wixsite.com/mypage>

**Copyright © 2028 Eric Yew Kee WONG.**

All right reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. For permission requests, write to the author, addressed "Attention: Permissions Coordinator," at the email below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

First printing edition 2028

email: [ericyewkeewong@gmail.com](mailto:ericyewkeewong@gmail.com)

# **TABLE OF CONTENTS**

## **PREFACE**

- On the Recurring Pattern of Accusation
- Scope and Methodology of This Study

## **PART I: INTRODUCTION — THE POLITICS OF TECHNOLOGICAL COMPETITION**

### **CHAPTER 1: THE ACCUSATION AS A REFLEX**

- 1.1 Defining the Phenomenon: When Competition Becomes Theft
- 1.2 The Central Thesis: Accusations as a Response to Lost Competitive Edge
- 1.3 Overview of Key Cases and Historical Precedents

### **CHAPTER 2: THE THEORETICAL FRAMEWORK**

- 2.1 Technological Hegemony and the Zero-Sum Mindset
- 2.2 The Weaponization of Intellectual Property Rhetoric
- 2.3 “AI Hegemonism” and the New Frontier of Accusation

## **PART II: HISTORICAL PRECEDENTS — AMERICA'S OWN PATH TO TECHNOLOGICAL POWER**

### **CHAPTER 3: THE UNITED STATES AS THE ORIGINAL TECHNOLOGY THIEF**

**3.1 Industrial Espionage in the Early Republic**

**3.2 Alexander Hamilton's "Report on Manufactures" (1791) and the  
Encouragement of Secret Acquisition**

**3.3 The Case of Samuel Slater: Memorizing British Textile Secrets**

**3.4 Francis Cabot Lowell and the Theft of the Power Loom Design**

**3.5 Scholarly Consensus: Doron Ben-Atar's Trade Secrets and  
America's Illicit Industrial Rise**

### **CHAPTER 4: FROM THIEF TO ENFORCER — THE HISTORICAL IRONY**

**4.1 The Transformation of American IP Policy**

**4.2 The Economic Espionage Act of 1996: Criminalizing What Built  
America**

**4.3 The First Federal Conviction Under the EEA: Walter Liew and the  
DuPont Case**

## **PART III: CONTEMPORARY CASES — AMERICA'S ACCUSATIONS IN THE MODERN ERA**

### **CHAPTER 5: THE HUAWEI CAMPAIGN — A DECADE OF ALLEGATIONS**

**5.1 The 2018 Indictment: Racketeering, Trade Secret Theft, and Iran Sanctions**

**5.2 The Meng Wanzhou Extradition Saga**

**5.3 Allegations of Theft from T-Mobile, Motorola, and Six U.S. Companies**

**5.4 The China Initiative (2018–2022) and Its Legacy**

**5.5 Huawei's Defense: "A Prosecutorial Target in Search of a Crime"**

### **CHAPTER 6: THE AI DISTILLATION CONTROVERSY — THE MOONSHOT AI CASE**

**6.1 The Rise of Moonshot AI and the Kimi K3 Model**

**6.2 White House Allegations: Covert Distillation of Anthropic's Fable Model**

**6.3 The Distillation Debate: Legitimate Technique or Intellectual Property Theft?**

**6.4 Treasury Secretary Bessent's Sanctions Threats**

**6.5 China's Response: Accusations of "AI Hegemonism" and Double Standards**

## **CHAPTER 7: THE DEEPSEEK PRECEDENT**

**7.1 DeepSeek's 2025 Breakthrough and the Immediate Accusations**

**7.2 The Pattern: Every Chinese AI Advance Triggers Theft Allegations**

**7.3 Knowledge Distillation as a Standard Industry Practice**

## **CHAPTER 8: OTHER HIGH-PROFILE CASES**

**8.1 Hytera Communications and the Motorola Trade Secrets Case**

**8.2 ZTE and U.S. Sanctions**

**8.3 The Section 301 Investigation and the "Forced Technology Transfer" Narrative**

## **PART IV: THE MECHANISM OF ACCUSATION**

## **CHAPTER 9: THE LEGAL AND POLICY ARCHITECTURE**

**9.1 The Special 301 Report: Annual Accusations Against China**

**9.2 The Entity List as a Geopolitical Weapon**

**9.3 Export Controls and the Semiconductor Embargo**

**9.4 Congressional Hearings and the Narrative of Chinese Theft**

## **CHAPTER 10: THE DOUBLE STANDARD EXPOSED**

**10.1 When American Labs Learn from Chinese Models: The Inkling Case**

**10.2 Forbes' Exposé: "When China Learns from U.S., It's Theft; When U.S. Learns from China, It's Engineering"**

**10.3 The Cursor-Moonshot Case: A U.S. Startup Built on Chinese Open-Source Technology**

**10.4 The Asymmetry of Rhetoric in AI Development**

## **CHAPTER 11: HISTORICAL PARALLELS — AMERICA'S PREVIOUS TARGETS**

**11.1 Japan in the 1980s: The IBM-Hitachi Espionage Case**

**11.2 The FBI Sting Operation and the Arrest of Japanese Engineers**

**11.3 The Toshiba-Kongsberg Scandal and the Soviet Connection**

**11.4 The Pattern: Accusing Strategic Competitors of Theft When They Threaten U.S. Dominance**

## **PART V: THE COUNTER-NARRATIVE — REBUTTALS AND CRITIQUES**

### **CHAPTER 12: CHINA'S OFFICIAL RESPONSES**

**12.1 The Commerce Ministry's Accusations of "AI Hegemonism"**

**12.2 China's White Paper on Forced Technology Transfer**

**12.3 The "Lack of Factual Basis and Legal Grounds" Argument**

**12.4 Threats of Retaliatory Measures**

### **CHAPTER 13: THE EXPERT AND SCHOLARLY CRITIQUE**

**13.1 Questioning the Evidence in the Section 301 Report**

**13.2 The Absence of Convincing Proof of Forced Technology Transfer**

**13.3 Industry Experts on the Normalcy of Knowledge Distillation**

**13.4 The Danger of Politicizing Technical Terminology**

### **CHAPTER 14: THE HYPOCRISY ARGUMENT**

**14.1 From "IP Thief to Hypocrite": The Historical Irony**

**14.2 America's Own History of Government-Sponsored Technology  
Theft**

**14.3 The Weaponization of Intellectual Property for Geopolitical Ends**

**14.4 Protecting Hegemony, Not Protecting Innovation**

## **PART VI: CONSEQUENCES AND IMPLICATIONS**

### **CHAPTER 15: IMPACT ON U.S.-CHINA RELATIONS**

**15.1 The Erosion of Bilateral Dialogue on AI Safety**

**15.2 Economic Decoupling and Supply Chain Disruption**

**15.3 The Risk of a Self-Defeating Strategy**

### **CHAPTER 16: IMPACT ON GLOBAL TECHNOLOGY AND INNOVATION**

**16.1 The Chilling Effect on Open-Source Collaboration**

**16.2 The Fragmentation of Global AI Development**

**16.3 The Cost to American Innovation and Competitiveness**

### **CHAPTER 17: THE FUTURE OF THE NARRATIVE**

**17.1 Will Accusations Intensify or Subside?**

**17.2 The Role of Open-Source Models in Defusing the Debate**

**17.3 Toward a New Framework for Global Technology Competition**

## **PART VII: CONCLUSION**

### **CHAPTER 18: SUMMARY OF FINDINGS**

**18.1 The Recurring Pattern: Accusation as a Response to Competitive Pressure**

**18.2 The Historical Irony: America's Own Origins in Technology Theft**

**18.3 The Double Standard: Asymmetrical Accusations in AI Development**

**18.4 The Geopolitical Function of Intellectual Property Rhetoric**

### **CHAPTER 19: FINAL REFLECTIONS**

**19.1 Innovation Cannot Be Contained by Borders**

**19.2 The Danger of Zero-Sum Thinking in Technology**

**19.3 A Call for Evidence-Based Dialogue**

## **APPENDICES**

**Appendix A: Timeline of Major U.S. Technology Theft Accusations  
(1982–2026)**

- Japan (1982) — IBM-Hitachi Case**
- China (2018) — Huawei Indictment**
- China (2025) — DeepSeek Distillation Accusations**
- China (2026) — Moonshot AI Case**

## **Appendix B: Key Legal Documents**

- **Economic Espionage Act of 1996 (18 U.S.C. §§ 1831–1839)**
- **Section 301 of the Trade Act of 1974**
- **USTR Special 301 Reports (Selected Excerpts)**

## **Appendix C: Glossary of Technical Terms**

- **Knowledge Distillation**
- **Model Extraction**
- **Forced Technology Transfer**
- **Entity List**
- **Export Controls**

## **Appendix D: Bibliography and Further Reading**

# **PREFACE**

## **On the Recurring Pattern of Accusation**

The accusation of technology theft has become one of the most persistent and consequential features of contemporary U.S.-China relations. From the Huawei indictments of 2018 to the DeepSeek distillation allegations of 2025 and the Moonshot AI controversy of 2026, a clear pattern has emerged: whenever a Chinese technological advance threatens to narrow or overturn America's perceived lead in a critical sector, allegations of intellectual property theft follow with remarkable consistency. This book argues that these accusations are not merely responses to evidence of wrongdoing but serve a deeper geopolitical function—they are a narrative response to competitive insecurity, a way of explaining away technological parity or defeat when American dominance falters.

Yet this pattern is not new. The United States itself rose to industrial prominence through systematic technology acquisition from Britain, often with governmental encouragement. The historical irony is profound: the nation that once celebrated Samuel Slater as the "Father of American Manufactures" for memorizing and smuggling British textile secrets now prosecutes foreign competitors under the very laws that would have criminalized its own founders. This book traces this arc from technology thief to global enforcer, examining how the weaponization of intellectual property rhetoric has become a primary tool of geopolitical competition in the twenty-first century.

## **Scope and Methodology of This Study**

This study examines American accusations of technology theft against strategic competitors from the early republic to the present day, with particular focus on the post-2018 escalation against China. It draws on primary legal documents, including indictments, statutes, and administrative reports; secondary historical scholarship; contemporary journalism and expert analysis; and official statements from both U.S. and Chinese government sources. The book employs a comparative historical methodology, identifying recurring patterns in American responses to technological competition from Britain, Japan, and now China.

The scope is deliberately broad, encompassing industrial espionage, trade secret theft, sanctions enforcement, and the emerging controversy over AI model distillation. By placing contemporary accusations in historical context, this study aims to illuminate not only what is being alleged but why such allegations emerge when they do—and what they reveal about American anxieties regarding the future of global technological leadership.

# **PART I: INTRODUCTION — THE POLITICS OF TECHNOLOGICAL COMPETITION**

## **CHAPTER 1: THE ACCUSATION AS A REFLEX**

### **1.1 Defining the Phenomenon: When Competition Becomes Theft**

The transformation of competitive technological achievement into allegations of theft represents a distinct rhetorical and political phenomenon. When a foreign competitor develops capabilities that rival or surpass American achievements, the default explanation in Washington increasingly frames that achievement as illegitimate—the product of theft rather than innovation. This phenomenon is observable across multiple domains: telecommunications with Huawei, semiconductors with various Chinese firms, and most recently artificial intelligence with DeepSeek and Moonshot AI.

The accusation reflex operates through a consistent logic: if American firms possess superior technology, and a foreign competitor achieves comparable results more quickly or efficiently, the only possible explanation—in this framing—is that the competitor must have stolen American intellectual property. This logic elides the possibility of independent innovation, efficient execution, or the cumulative nature of global scientific progress.

### **1.2 The Central Thesis: Accusations as a Response to Lost Competitive Edge**

This book advances a central thesis: American accusations of technology theft against strategic competitors are fundamentally responses to perceived or actual losses of competitive advantage. They function as a narrative defense mechanism—a way to preserve the myth of American technological exceptionalism in the face of evidence that the United States no longer possesses an unassailable lead in critical technologies.

The pattern is unmistakable. In the 1980s, as Japanese semiconductor and computer firms threatened American dominance, the FBI conducted sting operations against Japanese executives. In the 2010s and 2020s, as Chinese telecommunications and AI firms achieved global competitiveness, the Department of Justice launched sweeping prosecutions. In each case, the accusations intensified precisely as the competitive threat became most acute—not when the alleged theft occurred, but when the competitor's success became undeniable.

## **1.3 Overview of Key Cases and Historical Precedents**

This book examines a continuum of cases spanning more than two centuries. Part II explores America's own history as a technology thief in the early republic. Part III examines contemporary cases, including the Huawei campaign (Chapter 5), the Moonshot AI distillation controversy (Chapter 6), the DeepSeek precedent (Chapter 7), and other high-profile cases involving Hytera, ZTE, and Section 301 investigations (Chapter 8). Part IV analyzes the legal and policy architecture that enables these accusations, exposing the double standards that pervade American rhetoric. Part V presents the counter-narrative, including Chinese official responses and expert critiques. Part VI examines consequences and implications for U.S.-China relations and global innovation.

## **CHAPTER 2: THE THEORETICAL FRAMEWORK**

### **2.1 Technological Hegemony and the Zero-Sum Mindset**

The American approach to global technology competition is increasingly shaped by a zero-sum mindset—the belief that technological gains by competitors necessarily come at America's expense. This perspective treats technology as a finite resource rather than a cumulative, expanding domain of human knowledge. When combined with the assumption of American technological hegemony, this mindset produces a powerful cognitive bias: any challenge to American leadership must be explained as the result of unfair practices rather than legitimate competition.

This zero-sum framing has deep roots in American strategic culture but has intensified dramatically in the post-Cold War era, as the United States has sought to maintain unipolar dominance across all domains. In the technology sector, this has translated into an expansive interpretation of intellectual property rights and an aggressive enforcement posture that increasingly targets foreign competitors.

### **2.2 The Weaponization of Intellectual Property Rhetoric**

Intellectual property law, originally designed to incentivize innovation by granting temporary exclusivity, has been transformed into a geopolitical weapon. The rhetoric of intellectual property theft serves multiple functions: it delegitimizes foreign competition, justifies extraterritorial enforcement actions, mobilizes domestic political support for restrictive policies, and provides a moral framework for economic containment.

This weaponization operates through the strategic expansion of what counts as "theft." The concept has been stretched from the clear case of physical trade secret misappropriation to encompass practices like knowledge distillation—a standard technique in AI development—and even the normal process of learning from publicly available research. As one commentator observed, "It takes a concept familiar to any machine-learning practitioner and recasts it as a vehicle for theft".

## **2.3 "AI Hegemonism" and the New Frontier of Accusation**

The emergence of artificial intelligence as a critical technology has opened a new frontier in the politics of accusation. The concept of "AI hegemonism"—a term employed by Chinese officials in response to U.S. allegations—captures the perception that the United States seeks to monopolize AI development through a combination of export controls, sanctions, and rhetorical delegitimization of foreign achievements.

The AI context introduces novel complexities. Unlike traditional manufacturing or even semiconductor technology, AI models are built on open-source foundations, trained on publicly available data, and advanced through techniques like distillation that are openly discussed in academic literature. This makes the distinction between legitimate learning and illicit theft particularly fraught—and particularly susceptible to politicization.

## **PART II: HISTORICAL PRECEDENTS — AMERICA'S OWN PATH TO TECHNOLOGICAL POWER**

### **CHAPTER 3: THE UNITED STATES AS THE ORIGINAL TECHNOLOGY THIEF**

#### **3.1 Industrial Espionage in the Early Republic**

The United States did not achieve industrial dominance through purely organic innovation. As historian Doron S. Ben-Atar documents in his seminal work *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power*, "Americans stole much of the technology associated with the early industrial revolution, often with governmental support". During the colonial and revolutionary era, provincial and state governments actively encouraged the acquisition of European manufacturing knowledge through incentives to skilled immigrants.

This systematic technology acquisition was not merely tolerated but actively promoted by American leaders who understood that industrial development required access to European—particularly British—manufacturing secrets. The contradiction between America's later embrace of intellectual property protection and its origins in intellectual piracy is one of the great ironies of American economic history.

#### **3.2 Alexander Hamilton's "Report on Manufactures" (1791) and the Encouragement of Secret Acquisition**

Alexander Hamilton's *Report on the Subject of Manufactures*, presented to Congress on December 5, 1791, represents a foundational document in American industrial policy. In it, Hamilton argued for aggressive government support for manufacturing, including what Ben-Atar describes as essentially supporting "further technology piracy".

Hamilton understood that America could not wait for organic technological development; it needed to acquire existing knowledge from Europe. The report advocated for policies that would attract skilled artisans and manufacturers from abroad, including those possessing proprietary knowledge. This was not industrial espionage in the modern criminal sense—there was no American law against it—but it was a deliberate strategy of technology acquisition that Britain actively sought to prevent through laws banning the emigration of skilled workers and the export of machinery.

### **3.3 The Case of Samuel Slater: Memorizing British Textile Secrets**

Samuel Slater is perhaps the most famous example of early American technology theft. A textiles worker who learned pioneering mill techniques in Belper, Derbyshire, Slater broke British law by taking his knowledge across the Atlantic in 1789. He memorized designs and, disguising himself as a farmer, smuggled them to America.

To the British, Slater was "Slater the Traitor". To Americans, he became the "Father of the American Industrial Revolution". He established the first successful cotton mill in Pawtucket, Rhode Island, launching American textile manufacturing and establishing a pattern that would be repeated across multiple industries. As one commentator noted, "the story of Samuel Slater, from the early days of the United States, is just as much a tale of industrial espionage as its modern counterparts".

### **3.4 Francis Cabot Lowell and the Theft of the Power Loom Design**

Francis Cabot Lowell extended the pattern established by Slater. In 1810, Lowell traveled to Britain and spent months observing textile factories, memorizing the designs of power looms. Upon returning to America, he replicated the technology and established the Boston Manufacturing Company, launching the American factory system. Like Slater, Lowell was celebrated as an industrial pioneer—not prosecuted as a thief.

These cases illustrate a consistent pattern: technology that was "stolen" from Britain became the foundation of American industrial might, and the individuals responsible were celebrated as national heroes. The nation that would later criminalize such behavior under the Economic Espionage Act owed its industrial rise to the very practices it now condemns.

### **3.5 Scholarly Consensus: Doron Ben-Atar's Trade Secrets and America's Illicit Industrial Rise**

Ben-Atar's scholarship provides the definitive account of America's origins in intellectual piracy. His work "traces the evolution of America's contradictory approach to intellectual property rights from the colonial period to the age of Jackson". During the first decades of American independence, "private citizens, voluntary associations, and government officials encouraged the smuggling of European inventions and artisans to the New World".

Ben-Atar identifies several individuals who served as "American industrial spies in England in the 1780s and 1790s, attempting to convince skilled artisans to emigrate". Private organizations such as the Pennsylvania Society for the Encouragement of Manufactures and the Useful Arts actively encouraged similar behavior. This was not fringe activity but central to American economic development.

## **CHAPTER 4: FROM THIEF TO ENFORCER — THE HISTORICAL IRONY**

### **4.1 The Transformation of American IP Policy**

The transformation of the United States from technology thief to global intellectual property enforcer occurred gradually over the nineteenth and twentieth centuries. As American industry matured and American firms developed proprietary technologies worth protecting, the nation's attitude toward intellectual property shifted dramatically. The nation that had once celebrated the theft of British secrets began to demand international protection for its own innovations.

This transformation was completed in the late twentieth century, as the United States became the world's most aggressive advocate for intellectual property protection. The irony was not lost on observers: the nation that had built its industrial base through systematic technology acquisition now sought to criminalize the very practices that had made its rise possible.

### **4.2 The Economic Espionage Act of 1996: Criminalizing What Built America**

The Economic Espionage Act of 1996 (EEA), codified at 18 U.S.C. §§ 1831–1839, represents the culmination of America's transformation from technology thief to intellectual property enforcer. The Act criminalizes the theft or misappropriation of trade secrets, with enhanced penalties for offenses committed to benefit foreign governments.

The EEA effectively criminalized the practices that had built American industry. Samuel Slater, Francis Cabot Lowell, and the countless other Americans who had smuggled European technology to the New World would have been federal criminals under the EEA. The historical irony is profound: the law that now serves as the primary weapon against Chinese technology companies would have criminalized America's own founding industrialists.

### **4.3 The First Federal Conviction Under the EEA: Walter Liew and the DuPont Case**

The first federal jury conviction under the Economic Espionage Act came in the case of Walter Liew, convicted on March 6, 2014. Liew and his company, USA Performance Technology, Inc., were found guilty of conspiring to steal trade secrets from DuPont regarding chloride-route titanium dioxide production technology and selling those secrets to Chinese state-owned companies. He was sentenced to fifteen years in prison, ordered to forfeit \$27.8 million, and pay \$511,667.82 in restitution.

The Liew case established the EEA as a viable prosecution tool and set the stage for the broader campaign against Chinese technology companies that would follow. It also illustrated the geopolitical dimensions of trade secret enforcement: the prosecution was motivated not merely by private corporate interests but by concerns about Chinese industrial development.

## **PART III: CONTEMPORARY CASES — AMERICA'S ACCUSATIONS IN THE MODERN ERA**

### **CHAPTER 5: THE HUAWEI CAMPAIGN — A DECADE OF ALLEGATIONS**

#### **5.1 The 2018 Indictment: Racketeering, Trade Secret Theft, and Iran Sanctions**

The U.S. government's campaign against Huawei began in earnest with a January 2019 indictment that alleged the company had stolen trade secrets from T-Mobile, violated sanctions against Iran, and engaged in bank and wire fraud. A subsequent indictment in February 2020 added charges of racketeering and conspiracy, alleging that Huawei had been "basically stealing trade secrets from big American tech companies for two decades".

The indictment spelled out six different cases where employees of Huawei or its subsidiaries allegedly stole or attempted to steal technology. One case involved a Huawei employee accessing a robotics lab in Washington state and gathering information about a robot being developed by the company. Another involved a Huawei employee removing a robot arm from the lab, measuring and photographing it, and sending information back to Huawei management. Huawei acknowledged the incident but characterized it as isolated; the government presented it as part of a pattern.

#### **5.2 The Meng Wanzhou Extradition Saga**

The arrest of Huawei CFO Meng Wanzhou at Vancouver International Airport on December 1, 2018, at the request of the United States, became a major diplomatic flashpoint. The United States sought her extradition on fraud charges related to allegations that she had lied to HSBC about Huawei's relationship with its Iran-based affiliate Skycom.

The extradition case dragged on for years, becoming a symbol of the broader U.S.-China technology conflict. China repeatedly demanded Meng's release, accusing the United States of bullying and Canada of complicity in an unjust prosecution. The case illustrated how individual prosecutions could become instruments of geopolitical leverage.

### **5.3 Allegations of Theft from T-Mobile, Motorola, and Six U.S. Companies**

The Huawei indictments alleged theft from multiple American companies, including T-Mobile, Motorola, and Cisco. The T-Mobile case centered on a robot named "Tappy" designed to automatically test phones; prosecutors alleged that Huawei engineers secretly took photos of the robot, measured it, and attempted to steal parts of it from T-Mobile's lab in Washington state.

These allegations were part of a broader narrative that Huawei's success was built on intellectual property theft rather than legitimate innovation. However, critics noted that the cases often involved isolated incidents by individual employees rather than systematic corporate policy, and that Huawei had settled some disputes through licensing agreements.

### **5.4 The China Initiative (2018–2022) and Its Legacy**

The China Initiative, announced by the Department of Justice in 2018, represented a systematic effort to prosecute economic espionage and trade secret theft cases involving China. During its operation, the initiative generated over 2,000 investigations and prosecuted 148 individuals, 88% of whom were of Chinese ethnicity or Chinese nationals.

The initiative was widely criticized for racial profiling and for chilling academic exchange. It was formally ended in early 2022, with the Justice Department acknowledging that it had unfairly targeted Chinese-American scientists. However, many cases continued, and the initiative's legacy of suspicion and scrutiny persisted.

### **5.5 Huawei's Defense: "A Prosecutorial Target in Search of a Crime"**

Huawei consistently denied the allegations against it, arguing that it was being targeted for political reasons rather than genuine evidence of wrongdoing. The company's defense emphasized that it had invested heavily in research and development, held numerous patents, and contributed to global technology standards.

Critics of the U.S. campaign argued that the prosecution of Huawei was less about intellectual property theft than about containing Chinese technological ascent. The timing of the indictments—coinciding with the broader trade war and technology decoupling—suggested geopolitical motivations beyond the specific allegations.

## **CHAPTER 6: THE AI DISTILLATION CONTROVERSY — THE MOONSHOT AI CASE**

### **6.1 The Rise of Moonshot AI and the Kimi K3 Model**

Moonshot AI, a Beijing-based artificial intelligence startup backed by Alibaba and HongShan (formerly Sequoia China), emerged as a significant player in the global AI landscape with the release of its Kimi K3 model. The model attracted global attention for its strong performance in coding and agent-based benchmarks, with Moonshot claiming it could compete with leading systems developed by Anthropic and OpenAI.

The rapid advancement of Chinese AI models, following the earlier breakthroughs of DeepSeek, represented a direct challenge to American assumptions of AI supremacy. The response from Washington was swift and predictable.

### **6.2 White House Allegations: Covert Distillation of Anthropic's Fable Model**

On July 22, 2026, White House science adviser Michael Kratsios accused Moonshot AI of conducting a "large-scale" campaign to extract capabilities from American AI models, specifically alleging that Moonshot used Anthropic's Fable model to develop Kimi K3. Kratsios alleged that Moonshot created a "sophisticated internal platform to carry out model 'distillation' while rapidly switching between different methods of access to avoid detection".

The White House distinguished between legitimate research use of distillation and what it characterized as "large-scale, covert industrial distillation to steal American IP". Treasury Secretary Scott Bessent warned that sanctions and placement on the Commerce Department's Entity List would be considered.

### **6.3 The Distillation Debate: Legitimate Technique or Intellectual Property Theft?**

The Moonshot controversy centered on the practice of knowledge distillation—a standard technique in AI development through which "a less powerful AI system learns from the responses generated by a more advanced model". First popularized by computer scientist Geoffrey Hinton and his collaborators, distillation is "a compression technique that enables a smaller model—the 'student'—to learn from the outputs of a larger, more complex 'teacher'".

Industry experts pushed back against the U.S. allegations, pointing to the lack of evidence and arguing that distillation does not constitute intellectual property theft. Moonshot employee Randy Xian noted the narrow timeline—Fable 5 was released on July 1 and Kimi K3 on July 15—making it implausible that a brand new frontier model could have been trained in just 15 days through distillation.

### **6.4 Treasury Secretary Bessent's Sanctions Threats**

Treasury Secretary Scott Bessent's warnings that sanctions and Entity List placement would be considered against companies engaging in intellectual property theft represented an escalation of the administration's approach. "We support open-source AI and the innovation it unlocks," Bessent said. "But open source is not open season on American IP".

The threat of sanctions against Moonshot AI followed the established pattern of using trade restrictions as a tool of technology competition. However, critics noted that the allegations were made before any formal investigation or adjudication, suggesting a presumption of guilt rather than evidence-based enforcement.

### **6.5 China's Response: Accusations of "AI Hegemonism" and Double Standards**

China's Commerce Ministry responded by accusing the United States of "AI hegemonism" and threatening countermeasures. A ministry spokesperson stated that the U.S. was threatening Chinese tech companies "without factual or legal grounds".

The Chinese response framed the U.S. allegations as part of a broader pattern of attempting to maintain technological dominance through coercion rather than competition. The concept of "AI hegemonism" captured the perception that the United States sought to monopolize AI development and delegitimize any challengers.

## **CHAPTER 7: THE DEEPSEEK PRECEDENT**

### **7.1 DeepSeek's 2025 Breakthrough and the Immediate Accusations**

When DeepSeek achieved a major breakthrough in early 2025, American responses followed the established pattern. OpenAI and Google accused DeepSeek of intellectual property theft, claiming it had illegally trained on their models. OpenAI claimed to have evidence that DeepSeek had used distillation techniques to gain an advantage.

The DeepSeek case became a flashpoint in the broader debate over AI development and intellectual property. It illustrated how rapidly the U.S. response to Chinese AI advances had become reflexive: any significant achievement by a Chinese AI company would be met with allegations of theft.

### **7.2 The Pattern: Every Chinese AI Advance Triggers Theft Allegations**

The DeepSeek case established a clear pattern that would be repeated with Moonshot AI and others. As one commentator observed, "Amid protracted technological rivalry and political anxiety, there is a recurring temptation: to regard the normal working of innovation as evidence of conspiracy".

The pattern operates through a consistent logic: if a Chinese company achieves results comparable to American leaders, it must have stolen American technology. This logic is self-reinforcing—it becomes increasingly difficult to acknowledge Chinese innovation because doing so would undermine the assumption of American technological exceptionalism.

### **7.3 Knowledge Distillation as a Standard Industry Practice**

The DeepSeek controversy centered on knowledge distillation, which experts emphasized is "not a shadowy technique but one of AI's most widely understood and openly discussed methods". "It appears in academic papers, open-source repositories, and industry pipelines across continents".

As critics pointed out, "If learning from outputs constitutes theft, then much of modern science collapses into illegitimacy. Engineers routinely build on published results; models are benchmarked, compared, and improved through iterative refinement". The entire edifice of technological progress rests on this cumulative logic.

## **CHAPTER 8: OTHER HIGH-PROFILE CASES**

### **8.1 Hytera Communications and the Motorola Trade Secrets Case**

Hytera Communications, a Chinese telecommunications company, pleaded guilty in January 2025 to conspiracy to steal trade secrets from Motorola Solutions. The case involved the theft of thousands of Motorola's confidential documents and source code files. In February 2020, a jury had already found in favor of Motorola in its trade secret theft and copyright infringement case against Hytera.

The Hytera case resulted in a \$50 million fine and ongoing royalty obligations. Seven Hytera employees were indicted in 2021 for their alleged roles. The case followed the pattern of U.S. prosecutions targeting Chinese companies in strategic technology sectors.

### **8.2 ZTE and U.S. Sanctions**

ZTE, another Chinese telecommunications giant, was targeted in a similar case. The company was blacklisted and faced sanctions for allegedly violating U.S. export controls. The ZTE case illustrated the broader strategy of using sanctions and export controls to pressure Chinese technology companies, often based on allegations that were contested by the companies involved.

### **8.3 The Section 301 Investigation and the "Forced Technology Transfer" Narrative**

The Section 301 investigation of China's acts, policies, and practices related to technology transfer, intellectual property, and innovation resulted in tariffs and other measures. The investigation was based on allegations that China engaged in "forced technology transfer"—requiring foreign companies to share technology as a condition of market access.

Critics of the Section 301 report argued that the evidence was unconvincing. One analysis noted that "when it comes to the accusation that China engaged in forced technology transfer, the US indeed produced the purported evidence, the Section 301 Report," but the evidence was widely contested. Industry experts pointed out that technology transfer was often voluntary, part of normal business arrangements rather than government coercion.

# **PART IV: THE MECHANISM OF ACCUSATION**

## **CHAPTER 9: THE LEGAL AND POLICY ARCHITECTURE**

### **9.1 The Special 301 Report: Annual Accusations Against China**

The U.S. Trade Representative's annual Special 301 Report assesses intellectual property protection in trading partners. The 2025 report identified China as a Priority Foreign Country, citing "serious concerns" regarding technology transfer, trade secrets, counterfeiting, and online piracy. The report listed 26 trading partners, with eight—including China—placed on the Priority Watch List.

The Special 301 process functions as an annual ritual of accusation, establishing a baseline narrative of Chinese intellectual property violations that justifies ongoing enforcement actions.

### **9.2 The Entity List as a Geopolitical Weapon**

The Commerce Department's Entity List has become a primary tool of technology containment. Companies placed on the list face restrictions on accessing U.S. technology, effectively cutting them off from critical supplies and knowledge. Huawei, ZTE, and numerous other Chinese technology companies have been added to the list.

The Entity List functions as a geopolitical weapon because it can be deployed based on allegations rather than convictions, and because the consequences are severe enough to cripple targeted companies. As Bessent's warnings to Moonshot AI illustrated, the threat of Entity List placement is itself a tool of coercion.

### **9.3 Export Controls and the Semiconductor Embargo**

Export controls on advanced semiconductors represent perhaps the most consequential element of the U.S. technology containment strategy. By restricting Chinese access to advanced chips and chip-making equipment, the United States has sought to maintain a technological advantage in AI and other critical fields.

The semiconductor embargo has driven Chinese companies to develop domestic alternatives, accelerating rather than preventing Chinese technological development. It has also fragmented global supply chains and created uncertainty for American semiconductor companies.

### **9.4 Congressional Hearings and the Narrative of Chinese Theft**

Congressional hearings have played a crucial role in constructing and reinforcing the narrative of Chinese technology theft. Lawmakers have used hearings to amplify allegations, create a record of suspicion, and build political support for restrictive measures. The China Initiative itself was launched with significant congressional support.

The hearings function as a mechanism for translating allegations into policy, creating a feedback loop in which accusations generate political pressure for action, which in turn generates new accusations.

## **CHAPTER 10: THE DOUBLE STANDARD EXPOSED**

### **10.1 When American Labs Learn from Chinese Models: The Inkling Case**

The double standard in American rhetoric about technology learning was starkly illustrated by cases where American companies built on Chinese technology. When American labs learned from Chinese models, the practice was described as "engineering" or "innovation"; when Chinese labs learned from American models, it was described as "theft."

### **10.2 Forbes' Exposé: "When China Learns from U.S., It's Theft; When U.S. Learns from China, It's Engineering"**

Forbes captured this asymmetry in a widely cited observation: "When China learns from U.S., it's theft; when U.S. learns from China, it's engineering". The observation highlighted the rhetorical double standard that pervades American discourse on technology competition.

The asymmetry reflects a deeper assumption: American technology is legitimate and proprietary; Chinese technology is illegitimate and derived. This assumption allows American companies to freely build on Chinese innovations while accusing Chinese companies of theft for doing the same.

### **10.3 The Cursor-Moonshot Case: A U.S. Startup Built on Chinese Open-Source Technology**

The Cursor-Moonshot case provided a particularly stark illustration of the double standard. In March 2026, AI coding company Cursor launched Composer 2, which was built on Kimi K2.5, an open-source model from China's Moonshot AI. Cursor initially failed to disclose this, and was only discovered when users analyzed the underlying code.

The case demonstrated that American companies were actively building on Chinese AI technology—and that this was described as legitimate engineering, not theft. The asymmetry in rhetoric was impossible to ignore: when American companies used Chinese models, it was innovation; when Chinese companies used American models, it was theft.

## 10.4 The Asymmetry of Rhetoric in AI Development

The asymmetry in AI rhetoric extends beyond individual cases to the broader discourse. American commentators routinely describe Chinese AI advances as products of theft or copying, while describing American advances as products of innovation and creativity. This asymmetry serves to delegitimize Chinese achievements while celebrating American ones, regardless of the actual methods employed.

As one Chinese commentator noted, "The rhetorical asymmetry has now reached the point where it can no longer be ignored".

## **CHAPTER 11: HISTORICAL PARALLELS — AMERICA'S PREVIOUS TARGETS**

### **11.1 Japan in the 1980s: The IBM-Hitachi Espionage Case**

In June 1982, the FBI arrested six Japanese businessmen in a sting operation targeting Hitachi and Mitsubishi. The operation involved FBI agents posing as computer consultants selling IBM technical manuals. Hitachi admitted making \$540,000 in payments for IBM information.

The case was described as "possibly the largest industrial espionage case in history". It produced "deep embarrassment" in Japan "along with suspicion of United States motives and some soul-searching concerning the relative technological strengths of Japanese and American business".

### **11.2 The FBI Sting Operation and the Arrest of Japanese Engineers**

The FBI sting operation in the IBM-Hitachi case established a pattern that would be repeated with Chinese companies decades later. Undercover agents, sting operations, and aggressive prosecution were used to target foreign competitors. The arrests of Japanese executives sent a clear message: the United States would not tolerate challenges to its technological dominance.

### **11.3 The Toshiba-Kongsberg Scandal and the Soviet Connection**

The Toshiba-Kongsberg scandal of the 1980s involved the sale of advanced milling machines to the Soviet Union, enabling quieter submarine propellers. The case resulted in sanctions against Toshiba and contributed to the narrative of Japan as a threat to American security interests.

## **11.4 The Pattern: Accusing Strategic Competitors of Theft When They Threaten U.S. Dominance**

The pattern across these cases is unmistakable: when Japan threatened American dominance in semiconductors and computers in the 1980s, accusations of theft and espionage followed. When China threatens American dominance in telecommunications and AI today, the same pattern recurs.

This pattern suggests that the accusations are less about the specific conduct alleged and more about the competitive threat posed by the target. When a competitor becomes sufficiently threatening, allegations of theft provide a convenient narrative for explaining—and seeking to contain—that threat.

# **PART V: THE COUNTER-NARRATIVE — REBUTTALS AND CRITIQUES**

## **CHAPTER 12: CHINA'S OFFICIAL RESPONSES**

### **12.1 The Commerce Ministry's Accusations of "AI Hegemonism"**

China's Commerce Ministry has consistently rejected U.S. allegations, accusing the United States of "AI hegemonism" and threatening countermeasures. The ministry has stated that the U.S. is threatening Chinese tech companies "without factual or legal grounds".

The concept of "AI hegemonism" captures the Chinese perception that the United States seeks to monopolize AI development through coercion rather than fair competition. It frames U.S. actions not as legitimate enforcement but as an attempt to maintain dominance through illegitimate means.

### **12.2 China's White Paper on Forced Technology Transfer**

China has issued white papers and official statements rejecting allegations of forced technology transfer. These documents argue that technology transfer has been voluntary, part of normal business arrangements, and beneficial to all parties. They point to the lack of convincing evidence in the Section 301 report and other U.S. documents.

### **12.3 The "Lack of Factual Basis and Legal Grounds" Argument**

A consistent theme in Chinese responses is the argument that U.S. allegations lack factual basis and legal grounds. This argument emphasizes that the allegations are made before investigations are completed, that evidence is often circumstantial or absent, and that the legal theories employed (such as the criminalization of distillation) are novel and contested.

## **12.4 Threats of Retaliatory Measures**

China has threatened retaliatory measures in response to U.S. actions, including sanctions against American companies and restrictions on access to the Chinese market. These threats reflect the escalating nature of the technology conflict and the willingness of both sides to use economic leverage.

## **CHAPTER 13: THE EXPERT AND SCHOLARLY CRITIQUE**

### **13.1 Questioning the Evidence in the Section 301 Report**

Scholars and experts have questioned the evidence underlying the Section 301 report and other U.S. allegations. One analysis noted that the report's claims of forced technology transfer were based on "dated" examples and lacked convincing evidence. The report was criticized for making broad allegations without sufficient supporting documentation.

### **13.2 The Absence of Convincing Proof of Forced Technology Transfer**

The absence of convincing proof of forced technology transfer has been a recurring theme in expert critiques. Industry experts have pointed out that technology transfer is often voluntary, part of normal business arrangements, and that companies make their own decisions about what technology to share.

### **13.3 Industry Experts on the Normalcy of Knowledge Distillation**

AI industry experts have consistently pushed back against the characterization of distillation as theft. They emphasize that distillation is "one of AI's most widely understood and openly discussed methods" and that "the entire edifice of technological progress rests on this cumulative logic".

The global AI community "has pushed back against the Trump administration's claims that Moonshot AI's groundbreaking Kimi K3 distilled US models, citing a lack of justification and arguing that the practice does not constitute intellectual property theft".

### **13.4 The Danger of Politicizing Technical Terminology**

Experts have warned about the danger of politicizing technical terminology. As one commentator noted, "When a widely used engineering practice can be framed as a danger, the category itself risks becoming elastic to the point of meaninglessness". Policies built on such broad interpretations "tend to be blunt instruments, sweeping up benign activities alongside genuinely sensitive ones".

## **CHAPTER 14: THE HYPOCRISY ARGUMENT**

### **14.1 From "IP Thief to Hypocrite": The Historical Irony**

The historical irony of America's transformation from technology thief to intellectual property enforcer is a central theme of this book. The nation that built its industrial base through systematic technology acquisition now prosecutes others for the same practices. As one commentary noted, the United States has gone "from IP thief to hypocrite".

### **14.2 America's Own History of Government-Sponsored Technology Theft**

America's history of government-sponsored technology theft is well documented. From Alexander Hamilton's encouragement of technology piracy to the systematic acquisition of British manufacturing secrets, the U.S. government actively supported the theft of foreign technology. This history is not ancient—it continued through the nineteenth century and into the twentieth.

### **14.3 The Weaponization of Intellectual Property for Geopolitical Ends**

The weaponization of intellectual property for geopolitical ends represents a departure from the original purpose of intellectual property law. Rather than incentivizing innovation, intellectual property enforcement has become a tool of geopolitical competition, used to contain strategic competitors and maintain American dominance.

### **14.4 Protecting Hegemony, Not Protecting Innovation**

The argument that U.S. intellectual property enforcement is about protecting hegemony rather than protecting innovation is supported by the pattern of enforcement. The United States does not prosecute all intellectual property violators equally—it targets strategic competitors who threaten American dominance. The selective enforcement suggests geopolitical rather than principled motivations.

# **PART VI: CONSEQUENCES AND IMPLICATIONS**

## **CHAPTER 15: IMPACT ON U.S.-CHINA RELATIONS**

### **15.1 The Erosion of Bilateral Dialogue on AI Safety**

The escalating accusations and counter-accusations have eroded bilateral dialogue on AI safety and other areas of mutual concern. As cooperation has given way to competition, opportunities for joint governance of AI risks have diminished. The technology conflict has spilled over into other areas, poisoning the broader relationship.

### **15.2 Economic Decoupling and Supply Chain Disruption**

The technology conflict has driven economic decoupling, disrupting global supply chains and creating uncertainty for businesses. Export controls, sanctions, and tariffs have fragmented the global technology ecosystem, raising costs and reducing efficiency.

### **15.3 The Risk of a Self-Defeating Strategy**

There is a significant risk that the U.S. strategy will prove self-defeating. By restricting Chinese access to American technology, the United States has accelerated Chinese efforts to develop domestic alternatives. Export controls have created incentives for Chinese innovation rather than preventing it. The strategy may ultimately hasten the erosion of American technological leadership that it seeks to prevent.

## **CHAPTER 16: IMPACT ON GLOBAL TECHNOLOGY AND INNOVATION**

### **16.1 The Chilling Effect on Open-Source Collaboration**

The criminalization of practices like distillation has a chilling effect on open-source collaboration. If learning from publicly available models can be characterized as theft, the entire open-source ecosystem is threatened. Researchers may become reluctant to share their work for fear of being accused of facilitating theft.

### **16.2 The Fragmentation of Global AI Development**

The technology conflict has fragmented global AI development, creating separate American and Chinese ecosystems. This fragmentation reduces the benefits of global collaboration and may slow the overall pace of AI advancement.

### **16.3 The Cost to American Innovation and Competitiveness**

The U.S. strategy may ultimately harm American innovation and competitiveness. By restricting access to global talent and markets, by creating uncertainty for American companies doing business internationally, and by diverting resources to enforcement rather than innovation, the strategy may undermine American technological leadership.

## **CHAPTER 17: THE FUTURE OF THE NARRATIVE**

### **17.1 Will Accusations Intensify or Subside?**

The trajectory of accusations will likely depend on the trajectory of the technology competition. If Chinese AI continues to advance, accusations are likely to intensify. If the United States regains a clear lead, accusations may subside. The pattern from Japan in the 1980s suggests that accusations peak when the competitive threat is most acute.

### **17.2 The Role of Open-Source Models in Defusing the Debate**

Open-source models may play a role in defusing the debate over technology theft. If models are openly available, the distinction between legitimate use and theft becomes clearer. However, the U.S. has shown a willingness to characterize even open-source-based development as theft when it comes from Chinese competitors.

### **17.3 Toward a New Framework for Global Technology Competition**

A new framework for global technology competition is needed—one that recognizes the cumulative nature of technological progress, the legitimacy of learning from others, and the benefits of global collaboration. Such a framework would move beyond zero-sum thinking and embrace the possibility of mutual advancement.

## **PART VII: CONCLUSION**

### **CHAPTER 18: SUMMARY OF FINDINGS**

#### **18.1 The Recurring Pattern: Accusation as a Response to Competitive Pressure**

This book has documented a recurring pattern: American accusations of technology theft against strategic competitors intensify when those competitors threaten American dominance. The pattern is observable from Britain in the early republic to Japan in the 1980s to China today. The accusations are not merely responses to evidence but narrative responses to competitive insecurity.

#### **18.2 The Historical Irony: America's Own Origins in Technology Theft**

The historical irony is profound: the nation that now prosecutes technology theft built its industrial base through systematic technology acquisition from Britain, often with governmental encouragement. Samuel Slater, celebrated as the "Father of the American Industrial Revolution," was a technology thief by any modern definition.

#### **18.3 The Double Standard: Asymmetrical Accusations in AI Development**

The double standard in American rhetoric is stark: when American companies learn from Chinese models, it is described as "engineering" or "innovation"; when Chinese companies learn from American models, it is described as "theft". This asymmetry reflects a deeper assumption about the legitimacy of American versus Chinese technology.

## **18.4 The Geopolitical Function of Intellectual Property Rhetoric**

Intellectual property rhetoric serves a geopolitical function: it delegitimizes foreign competition, justifies extraterritorial enforcement, mobilizes domestic political support, and provides a moral framework for economic containment. The weaponization of intellectual property for geopolitical ends represents a departure from its original purpose of incentivizing innovation.

## **CHAPTER 19: FINAL REFLECTIONS**

### **19.1 Innovation Cannot Be Contained by Borders**

Innovation is a cumulative, global process. It cannot be contained by borders, export controls, or prosecutions. The attempt to monopolize technology is ultimately futile—and counterproductive. By attempting to contain Chinese innovation, the United States has accelerated it.

### **19.2 The Danger of Zero-Sum Thinking in Technology**

Zero-sum thinking in technology is dangerous. It leads to conflict rather than cooperation, fragmentation rather than integration, and ultimately to slower progress for all. A more productive approach would recognize that technological advancement is not a zero-sum game—gains by one nation do not necessarily come at the expense of others.

### **19.3 A Call for Evidence-Based Dialogue**

This book calls for evidence-based dialogue on technology competition—a dialogue that moves beyond reflexive accusations and acknowledges the complexity of global innovation. Such a dialogue would recognize the legitimacy of learning from others, the cumulative nature of technological progress, and the benefits of global collaboration. It would also acknowledge America's own history of technology acquisition and the double standards that pervade current rhetoric.

## **APPENDICES**

### **Appendix A: Timeline of Major U.S. Technology Theft Accusations (1789–2026)**

- 1789 — Samuel Slater memorizes British textile mill designs and smuggles them to America
- 1791 — Alexander Hamilton's Report on Manufactures encourages technology acquisition from Europe
- 1810 — Francis Cabot Lowell observes British power looms and replicates the technology in America
- 1982 — FBI sting operation targets Hitachi and Mitsubishi for alleged theft of IBM trade secrets
- 1996 — Economic Espionage Act enacted, criminalizing practices that built American industry
- 2014 — Walter Liew becomes first person convicted under the EEA
- 2018 — Huawei CFO Meng Wanzhou arrested in Canada at U.S. request
- 2018 — China Initiative launched by Department of Justice
- 2019 — Huawei indicted for trade secret theft and sanctions violations
- 2020 — Second Huawei indictment adds racketeering charges
- 2022 — China Initiative formally ended
- 2025 — DeepSeek breakthrough triggers distillation allegations
- 2025 — Hytera pleads guilty to conspiracy to steal Motorola trade secrets
- 2026 — Moonshot AI's Kimi K3 triggers White House distillation allegations
- 2026 — China accuses U.S. of "AI hegemonism" in response

## **Appendix B: Key Legal Documents**

### **Economic Espionage Act of 1996 (18 U.S.C. §§ 1831–1839)**

The Economic Espionage Act of 1996 criminalizes the theft or misappropriation of trade secrets. Section 1831 addresses economic espionage for the benefit of foreign governments; Section 1832 addresses theft of trade secrets for commercial purposes. The Act provides for significant criminal penalties, including imprisonment and fines.

The EEA represents the culmination of America's transformation from technology thief to intellectual property enforcer. The practices that built American industry—the systematic acquisition of foreign technology—would be criminal under the EEA.

#### **Key provisions:**

- 18 U.S.C. § 1831: Economic espionage (for foreign government benefit)
- 18 U.S.C. § 1832: Theft of trade secrets (commercial purposes)
- 18 U.S.C. § 1833: Exceptions (reverse engineering, independent derivation)
- 18 U.S.C. § 1834: Criminal forfeiture
- 18 U.S.C. § 1835: Confidentiality of trade secrets in court proceedings

### **Section 301 of the Trade Act of 1974**

Section 301 of the Trade Act of 1974 authorizes the U.S. Trade Representative to investigate and respond to foreign trade practices that are unfair or discriminatory. Section 301 investigations have been used to challenge Chinese practices related to technology transfer, intellectual property, and innovation.

The Section 301 process has been central to the U.S. technology containment strategy, providing the legal basis for tariffs and other measures against Chinese technology companies.

### **USTR Special 301 Reports (Selected Excerpts)**

The Special 301 Report is an annual review of intellectual property protection in U.S. trading partners. Countries with inadequate IP protection are placed on the Priority Watch List or Watch List.

2025 Special 301 Report — China identified as a Priority Foreign Country. The report cited "serious concerns" regarding "technology transfer, trade secrets, counterfeiting, online piracy, copyright law, patent and related policies, bad faith trademarks". Eight countries were placed on the Priority Watch List, including China.

## **Appendix C: Glossary of Technical Terms**

### **Knowledge Distillation**

Knowledge distillation is a machine learning technique through which a smaller model (the "student") learns from the outputs of a larger, more complex model (the "teacher"). First popularized by computer scientist Geoffrey Hinton and his collaborators, it is "a compression technique that enables a smaller model to learn from the outputs of a larger, more complex teacher".

Distillation has legitimate research and commercial applications and is "one of AI's most widely understood and openly discussed methods". It appears in academic papers, open-source repositories, and industry pipelines globally.

### **Model Extraction**

Model extraction (also called model stealing) refers to the process of replicating the functionality of a machine learning model through querying. While related to distillation, extraction typically implies obtaining the model's capabilities without authorization. The distinction between legitimate distillation and illicit extraction is contested and context-dependent.

### **Forced Technology Transfer**

Forced technology transfer refers to the alleged practice of requiring foreign companies to transfer technology as a condition of market access. The United States has alleged that China engages in forced technology transfer through joint venture requirements, licensing conditions, and administrative processes.

China has consistently denied these allegations, arguing that technology transfer is voluntary and part of normal business arrangements. Critics of the U.S. allegations have noted the absence of convincing evidence.

## **Entity List**

The Entity List is a U.S. Commerce Department list of foreign entities subject to export restrictions. Companies on the list face restrictions on accessing U.S. technology, including semiconductors, software, and other controlled items.

The Entity List has become a primary tool of technology containment, used to restrict Chinese access to critical technologies. Huawei, ZTE, and numerous other Chinese technology companies have been placed on the list.

## **Export Controls**

Export controls are restrictions on the export of sensitive technologies, including advanced semiconductors, AI software, and other dual-use technologies. The United States has implemented extensive export controls targeting China, restricting access to advanced chips and chip-making equipment.

Export controls have driven Chinese efforts to develop domestic alternatives, accelerating rather than preventing Chinese technological development.

## **Appendix D: Bibliography and Further Reading**

### **Books**

Ben-Atar, Doron S. *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power*. New Haven: Yale University Press, 2004.

Ben-Atar's seminal work documents America's origins in intellectual piracy, tracing "the evolution of America's contradictory approach to intellectual property rights from the colonial period to the age of Jackson". The book demonstrates that "Americans stole much of the technology associated with the early industrial revolution, often with governmental support".

### **Journal Articles**

Peskin, Lawrence A. "Review of *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power*." *Journal of American History* 92, no. 1 (June 2005): 201–202.

### **Government Documents**

U.S. Department of Justice. "Walter Liew Sentenced To Fifteen Years In Prison For Economic Espionage." Press Release, November 18, 2014.

U.S. Department of Justice. "Chinese Telecommunications Company Pleads Guilty to Conspiring To Steal Technology From Illinois-Based Motorola Solutions." Press Release, January 14, 2025.

U.S. Trade Representative. "2025 Special 301 Report." April 29, 2025.

## **News and Commentary**

BBC News. "British mill tycoon was a hero in the US but a traitor back home." June 28, 2026.

CGTN. "The fallout of US turning a technical term into a geopolitical weapon." April 26, 2026.

Reuters. "China accuses US of 'AI hegemonism', threatens countermeasures over potential probes." July 27, 2026.

South China Morning Post. "AI experts blast US claims of 'IP theft' by Moonshot's Kimi K3." July 23, 2026.

The Paper. "双标！中国AI被骂'偷'，美国照抄中国模型叫'工程'？" July 17, 2026.

## **Legal Sources**

18 U.S.C. §§ 1831–1839 (Economic Espionage Act of 1996)

Section 301 of the Trade Act of 1974

United States v. Walter Liew, 856 F.3d 585 (9th Cir. 2017)

**- THE END -**