China’s AI Espionage

National Intelligence Estimate

April 3rd, 2025

Written by: Stephen Roark

---

This estimate clearly outlines the potential security and economic risks surrounding Chinese cyber attacks and espionage within the U.S., with a specific focus on the rise of new artificial intelligence. It also provides future predictions if little to no action is taken and viable policy solutions to combat this issue.

**Introduction and Background**

Since 2000, China has been linked to 90 known intellectual property cyber espionage campaigns—30% more than Russia—with the actual number likely much higher. These campaigns have targeted a wide range of sectors, including defense contractors, semiconductor firms, and research universities, resulting in the systematic theft of trade secrets and sensitive innovation. Long-term effects of this have been detrimental to the American economy, with estimates running into billions of dollars worth of commercial and technological espionage. National security is similarly in jeopardy from the theft of weapon technology, data breaches, and malign influence. China’s growing espionage threat stems from the increasingly assertive and hostile nature of the Chinese Communist Party (CCP). While cyber attacks remain Beijing’s preferred method, which most of the time involves employing sophisticated hacking operations to access sensitive government, corporate, and research data, these digital tactics are far from the only tools in China’s arsenal. The CCP also relies on more

traditional espionage techniques, such as recruiting human assets through financial incentives or romantic entrapment, as well as unconventional methods, including the strategic purchase of property near sensitive military or research installations. The scope and scale of these espionage efforts are now supercharged by China’s rapid development and deployment of artificial intelligence. As digital tools become central to everything from economic infrastructure to democracy, China's infiltration into this realm threatens not just data security, but the broader stability of many major world actors.

The chart below illustrates the trend of publicly reported Chinese espionage cases over time. Notably, there is a visible decline following the 2015 agreement between President Obama and President Xi to curb government-led commercial cyber theft. However, that dip was short-lived as espionage activity surged again within a year. It's extremely important to note that the chart below is based on open-source material and likely does not reflect the actual number of incidents as China actively employs clandestine espionage operations that are left unnoticed.

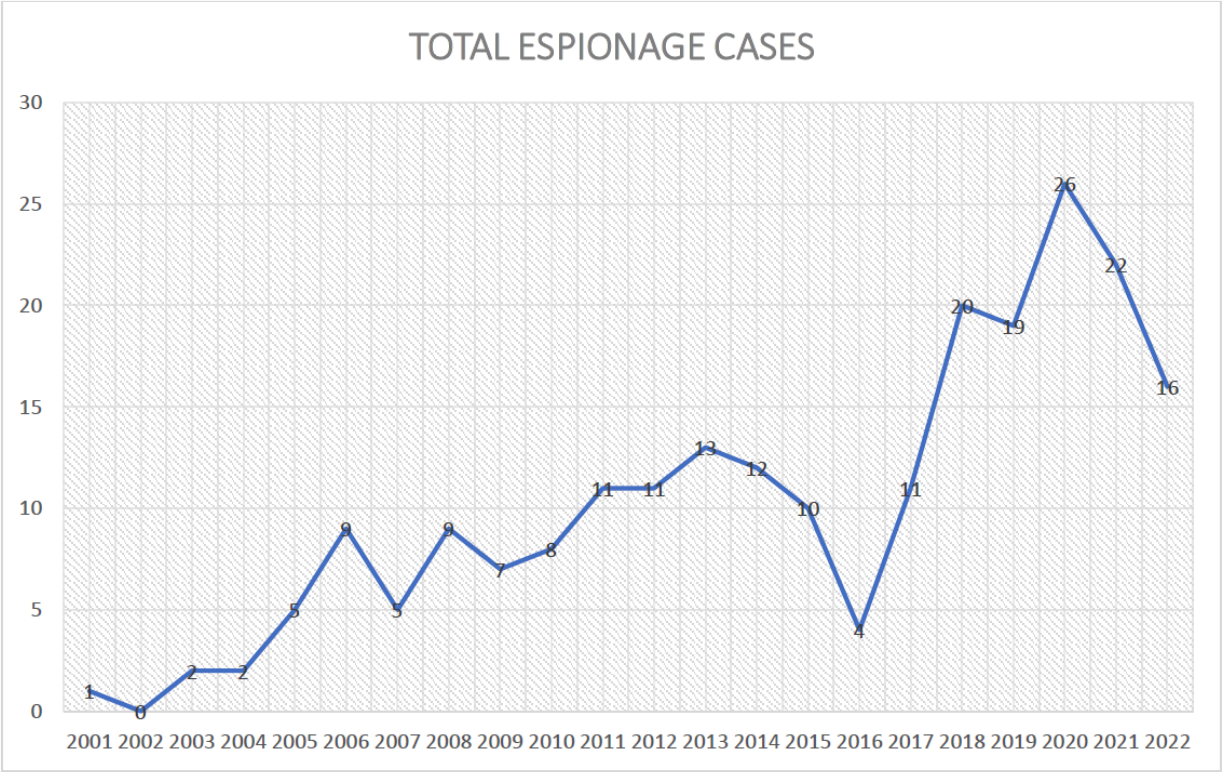


Photo: CSIS

A massive contributor to the uptick in Chinese cyber espionage can also be attributed to when Xi Jinping took office, first as Chair of the Central Military Commission in 2012, then General Secretary of the Chinese Communist Party in 2013. Cyber incidents in the United States greatly increased due to the Chinese Ministry of State Security gaining more responsibility over cyber capabilities. Given all of this and all other known data and intelligence, it is safe to declare that Chinese cyber capabilities, namely the advancement of AI and intelligized warfare, is the largest and most prominent threat the U.S. is facing right now and for the coming future.

**The Chinese Communist Party's Ambition**

A growing concern among U.S. intelligence officials is the CCP's vast aspirations for the future. Many of these plans and aspirations are intentionally made known through the release of public documents. There are two notable examples of such documents, that being the 2017 "New Generation AI Development Plan," and the "Military-Civil Fusion" doctrine of 2021.

Beginning with the 2017 document, a development plan for the next generation of artificial intelligence is outlined. 6 broad key tasks are identified in the document that deserve attention from the intelligence community, those tasks being: the fostering of innovation, the integration of AI into the economy, the integration of AI into society to facilitate convenience, military-civil fusion, building a secure and intelligent infrastructure system, and proactively planning the next generation of artificial intelligence projects. Based on these tasks, funding can be and is identified to specific sectors within the government, which is important to be aware of from a U.S. Intelligence standpoint. It is also worth noting the use of the word "brain" and "brain-inspired," which was mentioned many times and reflects China's view on the importance of the call to merge the interconnected human mind with that of AI. This is a particularly concerning idea as the effects of merging the two could be irreversible and have detrimental effects on how AI interacts with society across the globe. Recent surveys and data on Chinese AI-brain research support that this idea, expressed in 2017, has been underway. China is focusing heavily on the study of most "hard" problems the brain deals with, that being planning, continuous learning, creativity, sensemaking, and even intuition. Mathematical models are then made of the physical processes that produce these "hard" problems.

The technical term for this is “connectomics” or simply brain mapping. The idea the CCP is chasing is the eventual link of the two platforms, creating a system fully capable of artificial general intelligence (a machine that possesses the ability to understand or learn any intellectual task that a human being can).

Continuing with the 2021 doctrine, we see the CCP’s laid out strategy to develop the People’s Liberation Army into a "world class military" by 2049. Under this plan, Chinese science and technology departments were reorganized to warrant new innovations to also advance military development. Since the CCP believes that AI will drive the next revolution, in terms of military conflict and affairs, it is striving to be the first country to fully integrate AI to warfare (“intelligized warfare”). To achieve this, both licit and illicit strategies are being employed. These efforts span from strategic investments in private industries and global talent recruitment programs to the orchestration of academic and research partnerships aimed solely for military gain. These private industries and civilian firms are being increasingly authorized to conduct classified military research and weapons development. Example companies and industries under this effect are semiconductors, quantum computing, advanced nuclear technology, aerospace technology, and AI. The CCP also routinely engages in forced technology transfers, intelligence operations, and outright theft to accelerate and gain a technological edge. Furthermore, the CCP is taking advantage of the open, collaborative nature of the academic community—leveraging institutions like the China Scholarship Council, which compels scholarship recipients to report their overseas research activities directly to Chinese diplomatic missions, effectively turning academia into an extension of state intelligence. Overall, the military-civil fusion that China is

chasing is important as it directly threatens the trust and shared values that underscore international science and technology collaboration. The efforts being taken and the aspects laid out in this plan reflect the clandestine and non-transparent way the CCP is acquiring intellectual property and technological advancements, often illegally through trade secret theft, from researchers, scholars, and citizens.

Based on the above information and data, here are China's strategic goals boiled down:

- Undermine U.S. technological leadership.
- Support Chinese economic expansion by acquiring trade secrets.
- Influence public opinion in Western democracies through information operations.
- Strengthen the CCP's global soft power.
- Become a world-wide contender in cyber-space with cutting-edge A.I. developments.

**Case Study: DeepSeek**

With technology constantly evolving in 2025, China's activities in cyber constitute a fundamentally different and more urgent challenge to the U.S. today than they did a decade ago. The recent introduction of DeepSeek, a Chinese AI application, acts as a public display of China's cyber warfare over the last 10 years. With the app becoming the most downloaded free application in the country on Apple's app store, millions of Americans' user information is at risk; simultaneously, the extremely low-cost of the generative AI tool is creating economic implications for leading U.S. AI apps. Shares of Nvidia have dropped 17%, roughly $600 billion off its market value, with other manufacturers and apps trailing closely behind. American user data is at risk due to the

asymmetric advantage the CCP has over the U.S. in cyberspace with Chinese Law granting Beijing authority to access data from companies based in China. Data that could be used for behavior change campaigns, disinformation campaigns, and targeted messaging to Western audiences. Furthermore, the website and computer infrastructure of DeepSeek is owned by China Mobile, a Chinese state-owned telecommunications company that was banned from operating by the U.S. Federal Communications Commission in 2019 due to national security concerns.

Perhaps worth delving into more is the topic of data storage from this platform and others like it. Generative AI platforms like DeepSeek can create personalized disinformation at scale. They can synthesize credible-seeming news stories, deep fakes, and ideological content tailored to subgroups within U.S. society, which oftentimes can greatly misconstrue political thought and potential voting habits. Overall, this DeepSeek episode reveals a broader truth: China is using AI not just as a tool of espionage, but as an instrument of global influence and strategic advantage. The U.S. cannot afford to treat these threats as isolated incidents. Rather, they represent an intentional and accelerated effort by the Chinese state to shape digital world order.

**Case Study: Linwei Ding and Trade Secret Theft**

The one area, besides chip manufacturing, where China acknowledges a loss in is scientific ability and knowledge, which is offset by China's ability to tap into and steal from foreign sources, which is greatly difficult to control. For example, a former Google software engineer, Linwei Ding, was indicted in 2023 with stealing AI trade secrets from Google, for Chinese firms, whom he was secretly working for. Ding allegedly uploaded more than 1,000 files from Google and later circulated a PowerPoint presentation to

employees of a China based startup he founded. He was charged with seven counts each of economic espionage and theft of trade secrets; the trial/case is still ongoing.

This specific case exemplifies how China uses individual actors to extract more technologically advanced research from foreign countries, mainly the U.S. Similarly, it highlights the limitations of current U.S. counterintelligence efforts in detecting these insider threats in the private sector.

**Future Assessment**

Looking ahead and based on the documents released by the CCP, the cyber threat posed is not only expected to increase in volume but it is to become more integrated into Beijing's broader strategy. As the CCP advances its Military-Civil Fusion strategy, we can expect A.I systems to be weaponized at a rapid pace. The Intelligence Community needs to be concerned with China now beginning to set standards, rather than just catching up. If little to no action is taken:

- China will expand AI integration across all cyber espionage platforms by 2030.
- Tools like DeepSeek will proliferate and become increasingly embedded in U.S. networks.
- U.S. private sector dependency on AI tools, coupled with insufficient vetting mechanisms, will remain a core vulnerability.
- AI-generated disinformation will be used to disrupt elections, foster polarization, and manipulate U.S. public opinion.

**Proposed Policy Steps**

- Enforce stricter regulations on foreign AI applications operating in the U.S., requiring full transparency in data collection, storage, and access.

- Creating a centralized body of open source intelligence specialists within the U.S. government to monitor China's AI development as a whole, AI-brian research, and foreign acquisitions.
- Require U.S. app stores to include security warnings for applications associated with antagonistic foreign governments.
- Track and analyze Chinese cyber operations by mandating security assessments for AI apps that process large amounts of American user data.
- Evaluate outright banning DeepSeek, similar to previous actions against TikTok, if it poses a clear national security threat.
- Closely monitor for suspicious employee activity within large U.S. based tech companies and manufacturers.
- International agreements on A.I. use in military operations and application.

**Involved U.S. Agencies and Roles**

Several U.S. government and intelligence agencies–such as the CISA, NSA, FBI, NCSC, and FCC–need to engage in strengthening AI and data security regulations and banning or restricting high-risk applications. The agencies listed below have specific roles:

- NSA: Monitoring Chinese cyber activity through signals intelligence (SIGINT).
- FBI Cyber Division: More investigation and prosecution of domestic espionage cases.
- NCSC: Counterintelligence strategy and private-sector outreach.
- CISA: Protecting U.S. digital infrastructure.
- DoD: Developing offensive cyber deterrence capabilities.

- FCC: Enforcing bans on telecom firms like China Mobile.
- Commerce Department (BIS): Implementing export controls on AI chips and tools specifically used by China.

**Conclusion**

The integration of AI into China's cyber arsenal has amplified the speed, scale, and precision of its intelligence operations. This has enabled the ability for real-time surveillance, automated disinformation campaigns, and cyberattacks that can target critical infrastructure with minimal attribution risk. Moreover, China's strategy leverages both state-directed and civilian’s, blurring the lines between private and government control, and making it harder to detect and counter these threats through conventional means. As the CCP continues to embed AI into its military doctrine and industrial espionage, the U.S. must prepare for a fundamentally different era of geopolitical competition. An era where digital dominance could determine strategic outcomes across every domain, from the battlefield to the board meeting to the ballot box.

## Sources


国务院. “国务院关于印发新一代人工智能发展规划的通知_科技_中国政府网.” *Www.gov.cn*, 20 July 2017, www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

Kuo, Mercy A. “China’s Bid to Lead the World in AI.” *Thediplomat.com*, The Diplomat, 6 July 2024, thediplomat.com/2024/07/chinas-bid-to-lead-the-world-in-ai/.

*China AI-Brain Research*, cset.georgetown.edu/wp-content/uploads/CSET-China-AI-Brain-Research.pdf. Accessed 8 Apr. 2025.

*U.S. Department of State*, U.S. Department of State, www.state.gov/remarks-and-releases-bureau-of-international-security-and-nonproliferation/what-is-mcf-one-pager/. Accessed 7 Apr. 2025.

TAU, BYRON. “Researchers Raise Concerns about DeepSeek Chatbot’s Connection to Chinese Telecom.” *AP News*, 5 Feb. 2025, apnews.com/article/deepseek-china-generative-ai-internet-security-concerns-c52562f8c4760a81c4f76bc5fbdebad0.

Jensen, Benjamin. “How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy.” Www.csis.org, 19 Oct. 2023, www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy.

CSIS. “Survey of Chinese Espionage in the United States since 2000 | Strategic Technologies Program | CSIS.” Www.csis.org, 2023, www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

Stempel, Jonathan. “Ex-Google Engineer Faces New US Charges He Stole AI Secrets for Chinese Companies.” Reuters, 5 Feb. 2025, www.reuters.com/legal/ex-google-engineer-faces-new-us-charges-he-stole-ai-secrets-chinese-companies-2025-02-05/.

Metz, Cade. “OpenAI Uncovers Evidence of A.I.-Powered Chinese Surveillance Tool.” The New York Times, 21 Feb. 2025, www.nytimes.com/2025/02/21/technology/openai-chinese-surveillance.html.

Lyons, Emmet. “DeepSeek AI Raises National Security Concerns, U.S. Officials Say.” Cbsnews.com, CBS News, 28 Jan. 2025, www.cbsnews.com/news/deepseek-ai-raises-national-security-concerns-trump/.

Section 2: China’s Cyber Capabilities, www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf. Accessed 30 Mar. 2025.