

NSA, FBI and CISA warn of Chinese AI firms distilling US frontier models

Source copy kept by wheresthe.ai for the story "NSA, FBI and CISA warn of Chinese AI firms distilling US frontier models" (<https://wheresthe.ai/d/us-nsa-fbi-cisa-ai-distillation-advisory-2026-09/>).

Source: <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4592113/nsa-and-others-warn-china-based-ai-companies-are-distilling-us-frontier-ai-mode/>

Text saved 18 Oct 2026 (the page text through a reader, because the site refused a direct fetch).

SHA-256 of the saved text: 968dbccfa179cda54e4977a0caf0534752699436e4e9b991d8b2e6dcdbd4d68e6

PHOTO INFORMATION

FORT MEADE, Md. — Today, the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cybersecurity and Infrastructure Security Agency(CISA)released the Cybersecurity Advisory (CSA), ***China-Based Artificial Intelligence Companies Conducting Industrial-Scale Distillation Campaigns Against U.S. AI Companies.***

China-based artificial intelligence (AI) companies are engaging in aggressive, industrial-scale distillation activities that systematically extract restricted proprietary functionalities and capabilities of U.S. frontier AI models with the purpose of training their own, according to the report. While distillation is recognized as a legitimate and useful technique in AI research, China-based companies' use of distillation against U.S. models enables Chinese AI models to continually close the technology gap without expending high research and development costs and resources, including for compute, electricity, and foundational research, required for producing frontier AI models. Advances of Chinese AI models, consequently, enhances its military and cyberattack capabilities that could be used against the U.S. and our Allies.

This CSA provides background on AI knowledge distillation, how to detect if a model is being distilled, the sophisticated tactics, techniques, and procedures (TTPs) being used, and best practices for mitigation.

China-based AI companies deliberately distribute operations across the vast global AI ecosystem, including multiple AI model providers, cloud platforms, and infrastructure to avoid single-point detection. They also attempt to systematically distill the best capabilities and proprietary features of U.S. frontier models to train their China-based AI models. The U.S.-China competition in the frontier AI race has major national security implications since frontier AI models can pose significant risks to critical infrastructure, military, economic, and technology domains.

This activity impacts the public sector, industry, and foreign partner systems, as well as National Security Systems throughout the Defense Industrial Base and Department of War, either actively leveraging AI or adopting AI software or tools (such as large and small language models).

Collaboration across the broader AI ecosystem, including among cloud providers, application programming interfaces aggregators, and infrastructure providers, can enable coordinated defense against industrial-scale AI knowledge distillation campaigns. Cybersecurity analysts and other network defenders in the AI ecosystem are advised to use the guidance to detect any related activity and implement the listed mitigations to prevent these TTPs from being used successfully.

Read the report and visit our

full library for more cybersecurity information and technical guidance.

* * *

NSA Media Relations MediaRelations@nsa.gov 443-634-0721

* * *

About the National Security Agency

The National Security Agency leads the U.S. Government in cryptology that encompasses both foreign signals intelligence (SIGINT) insights and cybersecurity products and services and provides the Nation decision advantage in competition, crisis, and conflict.

###