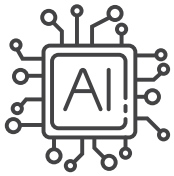
Free markets. Real solutions.

EXPLAINER

Open-Source AI in America: A Roadmap to Safeguarding U.S. Innovation and National Security

July 2025



China's bold claim that DeepSeek-R1 matched OpenAI's GPT-o1 model in reasoning capabilities while requiring significantly fewer computational resources raised urgent strategic questions.

The Open-Source AI Debate—Weighing Benefits and Risks

Open-source artificial intelligence (AI) has emerged as a distinct branch and increasingly strategic frontier of AI development. In contrast to closed-source AI, where the developing institution (e.g., corporation, academic lab, government) exclusively controls the training data, code, and models, open-source AI allows independent developers greater freedom to use, modify, study, and distribute key system components.

While open-source AI offers distinct benefits—such as lowering entry barriers for smaller firms and independent researchers, facilitating continuous learning and experimentation, and accelerating innovation through knowledge transfers—its high accessibility and transparency have sparked debate over its governance and deployment. Some skeptics argue that its "openness" complicates intellectual property enforcement, undermines data privacy, and weakens accountability. The potential for heightened cybersecurity risk is also a central concern, as researchers have already uncovered instances in which attackers exploited software vulnerabilities in publicly available training data, code scripts, and AI models to steal credentials, remotely control servers, and corrupt AI outputs. These trade-offs have prompted some companies to create "hybrid" approaches, such as controlled or tiered access, that aim to balance the benefits of openness with stronger cybersecurity resilience, oversight, and commercial viability.

Although these hybrid AI strategies are still evolving, their emergence underscores how navigating the open-source AI debate does not require an "all-or-nothing" approach. Rather, the path forward lies in crafting flexible solutions that mitigate the challenges and potential risks of open-source AI while unlocking its capacity to accelerate innovation at unprecedented speed and scale.

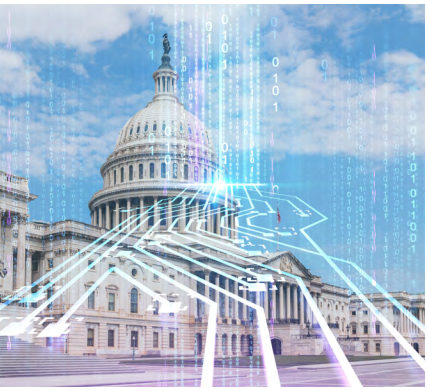
AI's "Sputnik" Moment—Past, Present, or Pending?

The release of DeepSeek's R1 model on Jan. 20, 2025 quickly captured the attention of policymakers and technologists across the United States, with many characterizing the event as AI's "Sputnik" moment. China's bold claim that DeepSeek-R1 matched OpenAI's GPT-o1 model in reasoning capabilities while requiring significantly fewer computational resources raised urgent strategic questions. Silicon Valley confronted the daunting possibility of a lasting shift away from proprietary innovation, while Washington, D.C. reevaluated the efficacy of export controls and debated the need for further regulatory oversight of open-source innovations.

In the months following DeepSeek-R1's release, China intensified its open-source AI momentum. A few notable recent releases include:

- *Baidu's ERNIE 4.5*: Initially touted as China's first major answer to America's ChatGPT, ERNIE 4.5 is now an open-source multimodal AI model with advanced capabilities in language understanding, visual processing, and complex reasoning tasks. This development underscores China's persistence in rivaling America's AI capabilities.
- *Huawei's Pangu Series*: Reflecting Huawei's transformation from telecom hardware to integrated AI solutions and specialized computing infrastructure, the Pangu series

Free markets. Real solutions.



If left unchecked and unchallenged, China's open-source AI initiatives could erode U.S. technological leadership and threaten national security.

Contact us

For more information, please contact:

Haiman Wong
Resident Fellow, Cybersecurity and Emerging Threats
hwong@rstreet.org

EXPLAINER

Open-Source AI in America: A Roadmap to Safeguarding U.S. Innovation and National Security

July 2025

provides industry-focused AI models targeting critical sectors like healthcare and finance, underscoring China's ambition to build comprehensive global AI ecosystems.

- *Rednote's dots.llm1*: Developed by Rednote, a popular Chinese social media platform previously seen as a promising TikTok alternative, dots.llm1 is an open-source large language model competitive with Alibaba's Qwen 2.5, highlighting China's broad investment into open-source AI.

China's aggressive push in open-source AI extends beyond mere technological ambition—it is a calculated move to embed its technologies, influence, standards, and values into the world's innovations and digital infrastructure. If left unchecked and unchallenged, China's open-source AI initiatives could erode U.S. technological leadership and threaten national security.

Moving Beyond the Debate—Policy Recommendations for Securing and Advancing Open-Source AI

While proprietary models still dominate U.S. AI development, private-sector initiatives like Meta's Llama models and OpenAI's highly anticipated open-source model have helped open-source AI gain meaningful traction. Policymakers can build on this momentum by positioning open-source AI as a national security priority. To guide its secure development and deployment, policymakers should also:

1. Establish clear, voluntary, and risk-based federal guidelines outlining best practices for securely deploying open-source AI.
2. Foster public-private partnerships dedicated to rigorous validation methods for AI models.
3. Implement risk-tiered liability shields to encourage innovation, especially for lower-risk open-source AI projects.
4. Invest in the development and integration of emerging technological solutions—such as embedded provenance tracking, AI-driven anomaly detection, and adaptive guardrails—to advance open-source AI security.
5. Promote industry-led best practices and licensing standards, such as copyleft agreements, to ensure community-driven accountability and sustained innovation.

Collectively, these recommendations chart a balanced path toward securing open-source innovation—not only as an immediate national security imperative, but as a strategic foundation for sustained U.S. leadership in emerging technological domains like AI agents and robotics.

Read More

- "Cyber and National Security Implications of America's AI Action Plan"
- "Mapping the Open-Source AI Debate: Cybersecurity Implications and Policy Priorities"
- "DeepSeek's cybersecurity failures expose a bigger risk. Here's what we really should be watching."
- "The Rise of AI Agents: Anticipating Cybersecurity Opportunities, Risks, and the Next Frontier"