THIRD WAY

REPORT *Published January 30, 2025 · 14 minute read*

Open-Source AI is a National Security Imperative

***Mike Sexton**, Senior Policy Advisor for Artificial Intelligence and Digital Technology*

Takeaways

America's footprint in artificial intelligence is prodigious, and it is hard to overstate how consequential this is for the American national interest if it further develops with the right balance between innovation and guardrails. Into this new technology are two divergent directions on the basic structure of the innovation: open-source or company controlled. ChatGPT is the latter model and was developed and licensed by OpenAI. Meta's LLaMa is an example of open-source AI. [1]

In this paper, we explore the benefits and drawbacks of open-source AI and conclude that open-source can help balance the safety and security we want from AI with the innovation necessary to set the standard for the world. Both models are right for innovation, safety, and competition.

- The increasing sophistication of AI raises concerns about risk. One of the chief issues is open-source AI, which a user can run without the developer's supervision.

- History shows us that the benefits of open-source software are real but diffuse and nebulous; meanwhile its greatest risks are tangible but mostly hypothetical.

- Encryption is an example of an open-source success. It is an open-source dual-use technology that vexes the US government. But accepting and adapting to it has been more farsighted than fighting it.

- Almost every smartphone in the world runs an American-made operating system thanks in large part to Android being open-source. We should not assume the development of open-source AI will necessarily follow the same trajectory.

- Open-source AI increases the likelihood that no single AI chatbot corners the consumer market and that America remains the innovation leader in AI.

What is "Open" AI?

Large language models are open-source when their code and weights can be downloaded and run with a license, without the developer's supervision (see: "What is 'Open' AI?"). Weights, also known as parameters, are numerical values that function like an LLM's neurons, encoding their "knowledge" and determining how they respond to queries. ChatGPT is the model you have most likely heard of, and it will soon be available with Siri, [2] but it is **not an open-source model,** meaning your Siri queries to ChatGPT will still have to be processed on OpenAI's servers.

Why? OpenAI was founded in 2015 as a nonprofit dedicated to open-source research into AI. [3] However, given its long-term goal to build **artificial general intelligence (AGI)**—an AI that can complete any task a human can [4] —its charter has long clarified that "safety and security concerns" [5] may prevent them from publishing some research in the future. That is, **OpenAI wasn't promising open-source AGI.**

Ilya Sutskever, cofounder and former chief scientist of OpenAI, has described AGI—which for now is only a concept—as "unbelievably potent." [6] To build such a powerful AI and **make it open-source** so anyone could use it without oversight was simply **too dangerous**.

While this reasoning may be sound, Apple had privacy concerns [7] and was reticent sharing its customers' data with a "nonprofit" whose legal structure is as straightforward as quantum mechanics. So when Siri and ChatGPT marry, your queries will be processed on OpenAI's servers—not Apple's. Apple anonymizes and encrypts requests *en route*, [8] but this privacy concern only arises for Apple customers because **ChatGPT is not open-source.**

Despite initial warnings about safety from OpenAI, open-source AI is becoming more common. Microsoft and Google respectively make the **open-source Phi** [9] **and Gemma** [10] models, which range from a petite 2 billion to a sturdy 27 billion parameters—a rough proxy for LLMs' complexity. But the **heavyweight champion of open-source AI in the US** is indisputably Meta, whose **largest open-source language model LLaMa 3.1** is available with a whopping 405 billion parameters.

Meta's **leadership in open-source AI** is an audacious gambit. OpenAI keeps its models under control for security, but subscriptions are also how it generates revenue. Meta offers comparably powerful **LLaMa** models for free (you pay to run it), shaping the AI landscape in its image but reaping no direct profits in the process. These two competing structures guarantee that no AI will become a pure monopoly, and LLaMa is already generating revenue for businesses incorporating it into their services and products. [11]

The monumentality of ChatGPT's launch evoked memories of the release of the original iPhone. [12] Extending this comparison, Meta's **LLaMa represents the Android of chatbots**. **What does it mean for Android and LLaMa to be open-source?** What are the attendant risks and benefits of these two general purpose technologies being available in the public domain, and what does it mean for America?

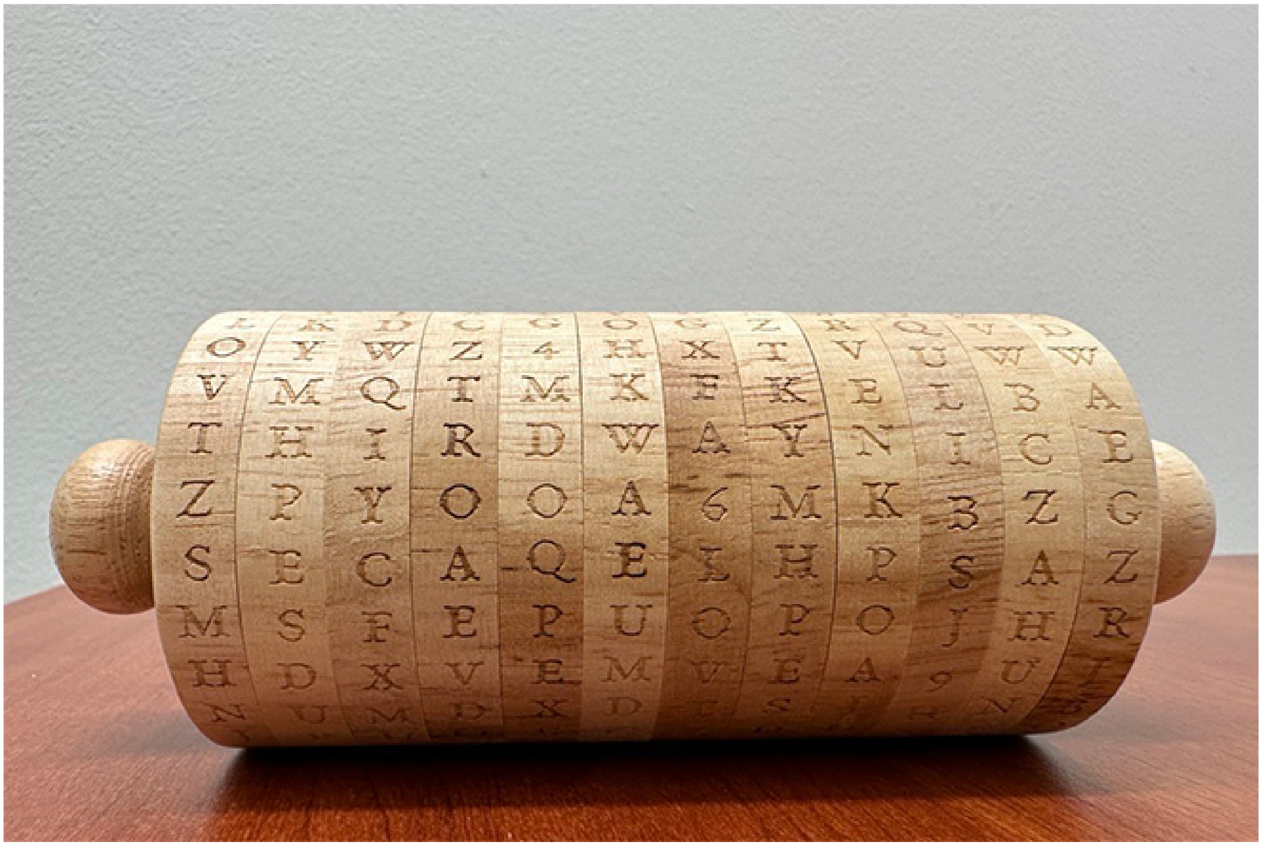
We will explore these implications as well as those related to cryptography, which has broadly been **open-source** since the National Bureau of Standards (now NIST—the National Institute of Standards and Technology) released the Data Encryption Standard in the 1970s. [13]

AI, like cryptography and smartphone operating systems, is a dual-use technology, meaning it can be used for civilian or military purposes, including by one's adversaries. Like the allegorical blind men struggling to identify an elephant by sense of touch, accurately accounting for the impacts of dual-use technologies is extremely challenging, as one can easily and correctly highlight their valid dangers without considering their countervailing benefits—or vice versa.

What We Can Learn from Open-Source Cryptography

Cryptography—the practice of scrambling information to render it indecipherable to anyone but its intended audience—is nearly as old as writing itself, beginning with ancient Egyptians substituting hieroglyphs to encrypt messages over a millennium before the common era. [14]

Governments and civilians contributed to cryptography's development. Thomas Jefferson developed a wheel of stacked wooden rings to encrypt messages as Secretary of State. [15] Edgar Allan Poe once wrote a challenge in a weekly messenger to break any substitution cipher sent to him—and evidently succeeded. [16] By the time Alan Turing cracked the Nazi's Enigma machine, cryptography had substantial momentum as a professional and academic discipline.



As the civilian computer age emerged, cryptography could no longer remain the domain of governments, militaries, and hobbyists. **A well-functioning computer-based society needed the means to communicate and store information securely.** This was not just a matter of privacy but of commerce, so in 1977 the Commerce Department's National Bureau of Standards (now NIST) released the **Data Encryption Standard (DES)** for public use. [17]

DES predates our contemporary notion of "open-source software," but cryptography's modern history as a primarily open discipline makes counterintuitive sense. A wunderkind who's built a new bulletproof encryption algorithm cannot simply sell it while keeping its workings secret: no investor worth their salt would trust it until the best professional cryptanalysts have attacked it, and that does not happen unless the algorithm is published. **It is the publicly known algorithms—those that experts have studied and attacked but still not broken—that are understood to be safest.**

Indeed, it was sunlight that eventually became DES's demise. While the algorithm began in IBM's labs, the company agreed with the US government to forfeit its patent and control of the development process for it to become a federal standard. In this process, it was not NIST but the NSA that pulled the strings, reducing the length of the encryption key to ensure it would not be too difficult to crack. [18] The key length gave DES a limited shelf life, and as computers became more advanced, secure protection required new algorithms with much longer keys.

What Does This Mean for Open-Source AI?

Just as open-source encryption algorithms are a public good, so too are open-source AI models like **LLaMa.** However, as with cryptography, democratizing knowledge entails doing so for "bad guys," too. Senators [19] and experts [20] have raised this concern regarding **LLaMa**, although **actual reports of LLaMa-enabled abuse can be counted on one hand.** But it is true: **LLaMa** is a possible tool in the toolkit of criminals, hackers, propagandists, and foreign spies who may have use for it—if not now then certainly in the future.

This problem is not unique to open-source models. Iran used closed-source ChatGPT for its election interference operations. (OpenAI and Microsoft thwarted the campaign, which received little traction.) [21] China's extensive experience hacking and spying to steal intellectual property [22] will also make it practically impossible to keep closed-source AI models secure from exfiltration indefinitely, especially from the AI replication technique known as "distillation." [23]

If an open-source model were abused to these ends, its open nature would make it harder to combat, but not impossible. The FBI [24] and US military [25] have a history of conducting cyber operations to shut down similarly illicit activity online.

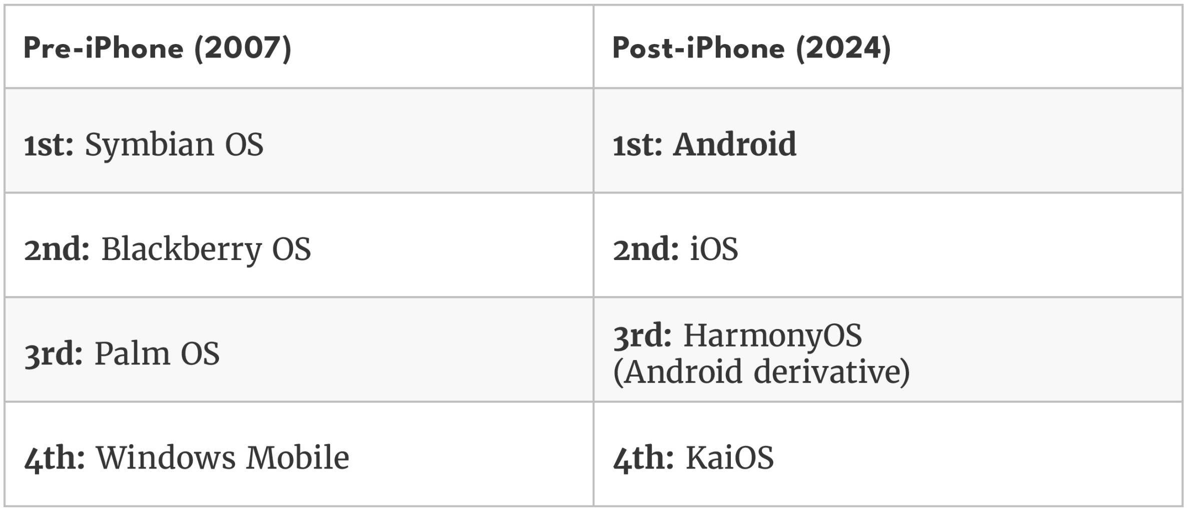
Being open-source gives LLaMa and other open models many advantages, too. LLaMA's 405 billion parameters are public, while the mere *number* of parameters in GPT-4 is a secret. [26] OpenAI's secretive approach to AI development makes sense in the historical context of nuclear fission research—an analogy well established in the public psyche. [27] Extending this analogy, **Meta, Google, and Microsoft's open-source approach is fulfilling the role of Atoms for Peace.**

Just as the best-known encryption algorithms are safest, the best-known AI models may be, too. [28] By open-sourcing **LLaMa**, Meta allows researchers and developers unlimited time to study the model and express how it can be improved, and Meta then can learn from their experience. **Open models' transparency, compared to closed-source competitors' default-to-secrecy approach, may define which models are considered the most ethically robust.** How can you be sure OpenAI is tweaking ChatGPT ethically if you never *see the weights*?

The US has effectively accepted and adapted to encryption. It relies on hacking tool companies to bypass secure smartphones in exigent circumstances [29] and is working diplomatically to improve the industry's standards of conduct. [30] The FBI and intelligence community's investigative capabilities remain robust, and Apple's right to build the most secure smartphones in the world remains intact. **Adapting to AI will not be easy for the US government, but if cryptography is a precedent, it is certainly possible.**

Androids ‘R’ Us

What made the iPhone release in 2007 so historic? Consider the most popular smartphone operating systems available on the eve of the iPhone’s release in 2007 and today:



Pre-iPhone (2007)	**Post-iPhone (2024)**
1st: Symbian OS	**1st: Android**
2nd: Blackberry OS	**2nd:** iOS
3rd: Palm OS	**3rd:** HarmonyOS (Android derivative)
4th: Windows Mobile	**4th:** KaiOS

Note: Source information does not capture 2007.
Source: “Mobile Operating System Market Share Worldwide.” StatCounter Global Stats, https://gs.statcounter.com/os-market-share/mobile/worldwide. Accessed 28 Jan. 2025.

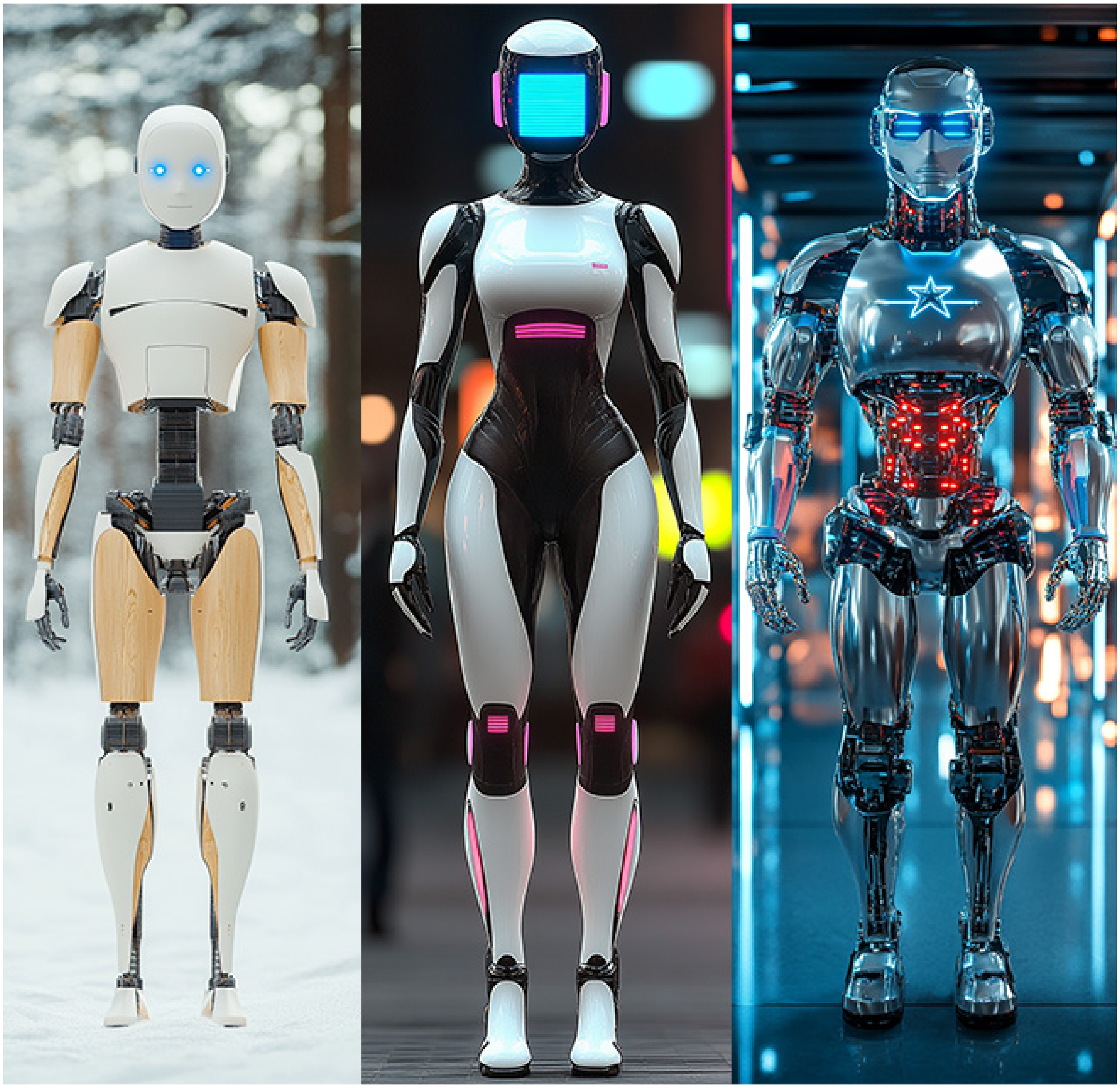
THIRD WAY

Before the iPhone, smartphones still featured vestiges of older internet-free cell phones: keyboards, dial pads, a pick-up and hang-up button. The iPhone and its closed-source iOS established the minimalist, pocket-sized black mirror as the smartphone archetype. The design change and norm of developer-friendly app stores went on to render every major smartphone operating system on the market in 2007 obsolete. **Android**, which became available in 2008, [31] gobbled up the remaining market share, becoming the dominant mobile OS with **3.9 billion users worldwide today.** [32]

How did the Android operating system come to reach nearly half the human population? By being open-source. Whereas Apple designed iOS for the iPhone, **Google designed Android for everyone**—in consortium with the **Open Handset Alliance**, which included device makers like Motorola and Samsung and chipmakers like Intel and Nvidia. [33] Android was a high-quality operating system that smartphone makers could use to build competitive devices at lower prices than Apple.

Today iOS and **Android** are effectively the only two smartphone operating systems. HarmonyOS, by Huawei, is closed-source and built upon **Android**; KaiOS is for budget phones with limited internet functionality, like WhatsApp. This is not necessarily the result of Google’s Machiavellian scheming: building a successful smartphone operating system requires massive resources and interaction with stakeholders, including a global community of app store developers.

By being open-source, **Android** has attracted the critical mass of developers needed for a flourishing app store. By being consensus-based, the platform has supported many smartphone manufacturers beyond just Google, including Samsung (S Korea), Motorola (US), Nokia (Finland), Xiaomi (China), and Oppo (China). **Android** epitomizes the rising tide lifting all boats, and **thanks to Android's open strategy, almost every smartphone in the world today runs an American-made operating system.**



Mobile operating systems and large language models are very different technologies, but both have seen American companies secure an early market lead. With the release of DeepSeek R1—a Chinese open-source model capable of planning and reasoning [34] —that advantage is in doubt. **If an AI model shaped by the Chinese Communist Party's ideology gains dominance in the global developer ecosystem, the consequences will be profound.** The balance of power between democracies and autocracies and the historical record of conquests past, present, and future hang in the balance.

AI: Made in America

It is much too early to tell, but if we take Android as precedent, **open-source American models like LLaMa, Phi, and Gemma can play a formative role in the global AI ecosystem.** All three are centrally available at huggingface.co, the top site for open-source AI models, with even more resources available at Ollama.com and LlamaIndex.com. What will this mean for America?

Being open-source gives LLaMa credibility—like Android's—with the developer community *worldwide*. Android followed iOS by 15 months; **LLaMa** followed ChatGPT by just three. As open-source models proliferate and get adopted, AI developers worldwide have far more incentive to build upon LLaMa than to reinvent the wheel, just as it makes more sense for mobile developers to build upon **Android** than replace it.

Chinese companies are not giving up the open-source AI race without a fight, however. DeepSeek's V3 and R1 models, which are respectively competitive with ChatGPT-4 and the "reasoning" model ChatGPT-o1, have stunned experts and erased over a trillion dollars from the stock market valuations of US tech giants. [35] Not only do DeepSeek's models perform extraordinarily well, but DeepSeek has also made them open-source [36] and documented that it can train models with far less resources than its American competition. [37]

That is why many experts see open-source AI development not as a risk, but as a national security *imperative.* [38] China seeks to influence the global AI ecosystem, and the open-source software ecosystem—the public toolbox for software developers worldwide—is a pivotal battleground. [39] The US has a vested interest in making sure the open-source programs that software developers weave into cyberspace and beyond are primarily made by America and its allies—not China.

Conclusion

We understand current events through historical analogy. The recent history informing American public sentiment toward AI can be traced to the US's loss to Huawei and China in the 5G race [40] and the spread of social media and its associated political tumult worldwide. Policymakers' attitudes toward AI tend to gravitate around two themes: 1) the imperative to outcompete China and 2) the prospect of catastrophic political and societal destabilization.

Competition with China is a powerful objective, but AI and 5G are different technologies with very different development trajectories. To paraphrase Chinese venture capitalist Kai-Fu Lee, American innovation pursues invention whereas Chinese innovation pursues perfection. China has not replicated the success of its 5G breakthrough in AI—the risk it is posing is instead in improving upon mimics of Western breakthroughs, as DeepSeek V3 [41] and R1 [42] have. This underscores why it is so important that the best open-source AI models in the world be American.

AI risks destabilizing human civilization just as social media did. How will we adjust to a world where intelligence is no longer scarce, or even human? No one knows, but **it matters that the inventors of these technologies are American.** We can criticize Android, Facebook, and ChatGPT, but they are not beholden to Xi Jinping.[43] Regardless of one's attitude toward these technologies, it is hard to imagine anyone sympathetic to democracy and freedom preferring them under the tutelage of the Chinese Communist Party.

The consequences of America's early dominance in the open development of AI may be more profound than its historic leadership in developing cryptography and mobile operating systems. The code in an encryption program or mobile operating system is explicable; the billions of parameters of a large language model are nearly inscrutable. **A backdoor in a smartphone is hard to find, but the liberal or capitalist parameters in an LLM are even more elusive.**

Some people will use open-source AI models for ill, just as criminals can avail themselves of smartphones with warrant-proof encryption. This is acknowledged by AI's most ecstatic champions[44] and it is not a trivial issue. **The better studied AI models—especially open models—are, the better platform providers and governments can get at spotting when they're abused.**

Navigating the future of AI requires situational awareness—not easy amid unprecedented change. While risks loom large, history reminds us that technological leadership is not predetermined but contested. With global competition intensifying, the stakes for America's AI ecosystem have never been higher. A singular focus on risk would be a mistake; securing America's global leadership in open-source AI is essential for national security.

TOPICS

ALL TOPICS

TECH AND AI 7

ENDNOTES

[1] We acknowledge and elect not to abide by the strict definition of “open source AI” created by the Open Source Initiative, which requires models’ training data to be public to be considered open-source. The colloquial and tenuously understood meaning of “open-source software” is of publicly available code that a developer can copy, edit, and run—a semantic category which has obvious implications with respect to AI. We chose not to complicate this argument with either a peripheral digression about training data or with less accessible terminology like “open *weight* AI.”
“The Open Source AI Definition — by The Open Source Initiative.” *Open Source Initiative*, https://opensource.org/ai. Accessed 18 Nov. 2024.

[2] “OpenAI and Apple Announce Partnership.” *OpenAI*, 10 June 2024, https://openai.com/index/openai-and-apple-announce-partnership/. Accessed 30 September 2024.

[3] Brandom, Russell. “Elon Musk and Partners Form Nonprofit to Stop AI from Ruining the World.” *The Verge*, 11 Dec. 2015, https://www.theverge.com/2015/12/11/9910742/elon-musk-openai-sam-altman-y-combinator-machine-learning. Accessed 30 September 2024.

[4] Hashemi-Pour, Cameron, and Ben Lutkevich. “What Is Artificial General Intelligence? Definition from TechTarget.” *Enterprise AI*, https://www.techtarget.com/searchenterpriseai/definition/artificial-general-intelligence-AGI. Accessed 30 September. 2024.

[5] “OpenAI Charter.” *OpenAI*, https://openai.com/charter/. Accessed 30 September. 2024.

[6] Vincent, James. “OpenAI Co-Founder on Company’s Past Approach to Openly Sharing Research: ‘We Were Wrong.’” *The Verge*, 15 Mar. 2023, https://www.theverge.com/2023/3/15/23640180/openai-gpt-4-launch-closed-research-ilya-sutskever-interview. Accessed 30 September 2024.

7. Edu, Jide. “Apple Insists Its ChatGPT Tie-up Will Protect Users’ Privacy: Here Are the Questions It Must Answer First.” *The Conversation*, 14 June 2024, http://theconversation.com/apple-insists-its-chatgpt-tie-up-will-protect-users-privacy-here-are-the-questions-it-must-answer-first-232498. Accessed 2 October 2024.

8. O’Flaherty, Kate. “Apple Intelligence Is Coming. Here’s What It Means for Your iPhone.” *The Observer*, 24 Aug. 2024. *The Guardian*, https://www.theguardian.com/technology/article/2024/aug/24/apple-intelligence-iphone-ios-18-siri-chat-gpt-launch. Accessed 30 September 2024.;

9. Bilenko, Misha. “Introducing Phi-3: Redefining What’s Possible with SLMs.” *Microsoft Azure Blog*, 23 Apr. 2024, https://azure.microsoft.com/en-us/blog/introducing-phi-3-redefining-whats-possible-with-slms/. Accessed 30 September 2024.

10. “Google AI Gemma Open Models | Google for Developers.” *Google AI for Developers*, https://ai.google.dev/gemma. Accessed 30 Sept. 2024.

11. Paul, Katie. “Meta Says Its Llama AI Models Being Used by Banks, Tech Companies | Reuters.” *Reuters*, 29 Aug. 2024, https://www.reuters.com/technology/artificial-intelligence/meta-says-its-llama-ai-models-being-used-by-banks-tech-companies-2024-08-29/. Accessed 2 October 2024.

12. Coyne, Alan. “iPhone VS ChatGPT...Is ChatGPT Having an ‘iPhone Moment’?” *UCD Professional Academy*, https://www.ucd.ie/professionalacademy/resources/iphone-vs-chatgpt/. Accessed 2 Oct. 2024.

13. Schneier, Bruce. “The Legacy of DES - Schneier on Security.” *Schneier on Security*, 6 Oct. 2004, https://www.schneier.com/blog/archives/2004/10/the_legacy_of_d.html. Accessed 30 September 2024.

14. Dorman, Peter F., and Hellmut Brunner. “Hieroglyphic Writing - Cryptography, Ancient Egypt, Symbols | Britannica.” *Britannica*, https://www.britannica.com/topic/hieroglyphic-writing/Cryptographic-hieroglyphic-writing. Accessed 1 Oct. 2024.

15. "Wheel Cipher." *Monticello*, https://www.monticello.org/research-education/thomas-jefferson-encyclopedia/wheel-cipher/. Accessed 1 Oct. 2024.

16. Morelli, R. "Poe and Cryptography." *Trinity College*, 3 May 2018, http://www.cs.trincoll.edu/~crypto/historical/poe.html. Accessed 1 October 2024.

17. Burr, W. E. "Data Encryption Standard." National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/sp958-lide/250-253.pdf. Accessed 1 October 2024.

18. Levy, Steven. *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age.* Viking, 2001. Pages 52-66.

19. "Hawley and Blumenthal Demand Answers from Meta, Warn of Misuse After 'Leak' of Meta's AI Model." *Josh Hawley*, 6 June 2023, https://www.hawley.senate.gov/hawley-and-blumenthal-demand-answers-meta-warn-misuse-after-leak-metas-ai-model/. Accessed 2 October 2024.

20. Perrigo, Billy. "Mark Zuckerberg Just Intensified the Battle for AI's Future." *TIME*, 24 July 2024, https://time.com/7002563/mark-zuckerberg-ai-llama-meta-open-source/. Accessed 2 October 2024.

21. Kim, Juliana. "OpenAI Says Iranian Group Using ChatGPT Tried to Sow Division Ahead of U.S. Election." *NPR*, 17 Aug. 2024. *NPR*, https://www.npr.org/2024/08/17/nx-s1-5079397/openai-chatgpt-iranian-group-us-election. Accessed 2 October 2024.

22. Flannery, Russell. "China Theft Of U.S. Information, IP One Of Largest Wealth Transfers In History: FBI Chief." *Forbes*, 7 July 2020, https://www.forbes.com/sites/russellflannery/2020/07/07/china-theft-of-us-information-ip-one-of-largest-wealth-transfers-in-history-fbi-chief/. Accessed 23 January 2024.

23. Schechner, Sam. "OpenAI Investigating If China's DeepSeek Used Its Models to Train New Chatbot - WSJ." *The Wall Street Journal*, 29 Jan. 2025, https://www.wsj.com/tech/ai/openai-china-deepseek-chatgpt-probe-ce6b864e?mod=hp_lead_pos2. Accessed 29 January 2025.

24. "Office of Public Affairs | Criminal Marketplace Disrupted in International Cyber Operation." *US Department of Justice*, 5 Apr. 2023, https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation. Accessed 8 October 2024.

25. Nakashima, Ellen. "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms - The Washington Post." *The Washington Post*, 27 Feb. 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html. Accessed 8 October 2024.

26. Horwath. "Number of Parameters in GPT-4 (Latest Data)." *Exploding Topics*, 6 Aug. 2024, https://explodingtopics.com/blog/gpt-parameters. Accessed 4 October 2024.

27. Weil, Elizabeth. "Who Is OpenAI's Sam Altman? Meet the Oppenheimer of Our Age." *New York Magazine*, 25 Sept. 2023, https://nymag.com/intelligencer/article/sam-altman-artificial-intelligence-openai-profile.html. Accessed 2 October 2024.

28. Kapoor, Sayash, et al. "On the Societal Impact of Open Foundation Models." *Stanford Center for Research on Foundation Models*, Dec. 2023, https://crfm.stanford.edu/open-fms/. Accessed 4 October 2024.

29. Mazzetti, Mark, and Ronen Bergman. "Lawmakers Signal Inquiries Into U.S. Government's Use of Foreign Spyware." *The New York Times*, 28 Dec. 2022. *NYTimes.com*, https://www.nytimes.com/2022/12/28/us/politics/spyware-israel-dea-fbi.html. Accessed 5 October 2024.

30. House, The White. "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware." *The White House*, 18 Mar. 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/. Accessed 5 October 2024.

31. Berne, Philip. “The First Android Is 15 Years Old, and It Is the Opposite of Everything We Want in a Smartphone Today.” *TechRadar*, 23 Sept. 2023, https://www.techradar.com/phones/the-first-android-is-15-years-old-and-it-is-the-opposite-of-everything-we-want-in-a-smartphone-today. Accessed 4 October 2024.

32. AppMySite. “Android vs iOS: Mobile Operating System Market Share Statistics (Updated 2024).” *AppMySite*, 29 June 2022, https://www.appmysite.com/blog/android-vs-ios-mobile-operating-system-market-share-statistics-you-must-know/. Accessed 4 October 2024.

33. “Android | Definition, History, & Facts | Britannica.” *Britannica*, 30 Sept. 2024, https://www.britannica.com/technology/Android-operating-system. Accessed 4 October 2024.

34. Citation: “Deepseek-Ai/DeepSeek-R1.” 2025. Reprint, DeepSeek, January 29, 2025. https://github.com/deepseek-ai/DeepSeek-R1. Accessed 29 January 2025.

35. Matchett. “Nvidia Stocks: DeepSeek AI Launch Sees $1tn Wiped off World’s Biggest Tech Companies.” *The Independent*, 28 Jan. 2025, https://www.independent.co.uk/business/deepseek-ai-nvidia-meta-google-share-price-news-b2687448.html. Accessed 28 January 2025.

36. *Deepseek-Ai/DeepSeek-R1*. 2025. DeepSeek, 28 Jan. 2025. *GitHub*, https://github.com/deepseek-ai/DeepSeek-R1. Accessed 28 January 2025.

37. “DeepSeek-V3 Technical Report.” *Arxiv*, 27 Dec. 2024, https://arxiv.org/html/2412.19437v1. Accessed 28 January 2025.

38. McBride, Keegan. “Open Source AI: The Overlooked National Security Imperative.” *Just Security*, 6 June 2024, https://www.justsecurity.org/96422/open-source-ai-the-overlooked-national-security-imperative/. Accessed 18 November 2024.

39. Ball, Keegan McBride, Dean W. “The United States Must Win The Global Open Source AI Race.” *Just Security*, 7 Nov. 2024, https://www.justsecurity.org/104676/american-ai-leadership-requires-support-open-source/. Accessed 18 November 2024.

40. Sacks, David. “China’s Huawei Is Winning the 5G Race. Here’s What the United States Should Do To Respond | Council on Foreign Relations.” *Council on Foreign Relations*, 29 May 2023, https://www.cfr.org/blog/china-huawei-5g. Accessed 6 October 2024.

41. DeepSeek-AI, Aixin Liu, Bei Feng, Bing Xue, Bingxuan Wang, Bochao Wu, Chengda Lu, et al. “DeepSeek-V3 Technical Report.” Python, January 29, 2025. https://github.com/deepseek-ai/DeepSeek-V3. Accessed 29 January 2025.

42. “Deepseek-Ai/DeepSeek-R1.” 2025. Reprint, DeepSeek, January 29, 2025. https://github.com/deepseek-ai/DeepSeek-R1. Accessed 29 January 2025.

43. Singleton, Craig. “It’s Not Just a Theory. TikTok’s Ties to Chinese Government Are Dangerous.” *FDD*, 18 Mar. 2024, https://www.fdd.org/analysis/2024/03/18/its-not-just-a-theory-tiktoks-ties-to-chinese-government-are-dangerous/. Accessed 6 October 2024.

44. Andreessen, Marc. “Why AI Will Save the World.” *Andreessen Horowitz*, 6 June 2023, https://a16z.com/ai-will-save-the-world/. Accessed 5 October 2024.