The National Security Case for Public AI

Vanderbilt
Policy Accelerator
for Political Economy & Regulation

VANDERBILT UNIVERSITY

Vanderbilt
Policy Accelerator
for Political Economy & Regulation

About the Vanderbilt Policy Accelerator

The Vanderbilt Policy Accelerator focuses on cutting-edge topics in political economy and regulation to swiftly bring research, education, and policy proposals from infancy to maturity.

About the Authors

Ganesh Sitaraman holds the New York Alumni Chancellor's Chair in Law at Vanderbilt Law School and is the Director of the Vanderbilt Policy Accelerator. He is the author of five books, including Networks, Platforms, and Utilities: Law and Policy (2022) (with Morgan Ricks, Shelley Welton, & Lev Menand) and The Public Option (Harvard University Press, 2019) (with Anne Alstott). He is a public member of the Administrative Conference of the United States. He teaches and writes about constitutional law, the regulatory state, economic policy, democracy, and foreign affairs.

Alex Pascal is a Senior Fellow at the Ash Center for Democratic Governance and Innovation and a Professor of Practice at the Fletcher School of Law and Diplomacy at Tufts University. Alex has served for over a decade as a national security and domestic policymaker in the United States Government, including seven years at the White House. His current research focuses on governance and policy for artificial intelligence.

Acknowledgements: The authors thank Ramsay Eyre, Joel Dodge, Amba Kak, Mara Karlin, Grace May, Jim Mitre, Jim Miller, and Brett Rosenberg for helpful suggestions. This paper was partly supported by funding from the Mozilla Foundation.

Table of Contents

Introduction

In a recent op-ed in the *Washington Post*, OpenAI CEO Sam Altman posed a simple but striking question: "Who will control the future of AI?" Altman frames the choice as between two futures: "Will it be one in which the United States and allied nations advance a global AI that spreads the technology's benefits and opens access to it, or an authoritarian one, in which nations or movements that don't share our values use AI to cement and expand their power? There is no third option—and it's time to decide which path to take."[1] Implicit in Altman's binary framing is that Silicon Valley and companies like his own are our democratic bulwark against a techno-authoritarian future in which China is predominant.

National security and foreign policy arguments like this one have become increasingly common in AI and technology policy conversations. The basic contours of the argument go something like this: The United States needs – and should depend on – its leading companies to maintain the AI innovation edge and establish dominance in AI in order to win the global competition with China. Anything that might restrain these leading companies (i.e. regulation, antitrust enforcement, or other government actions in the space—with the notable exception of massive public R&D investment that American industry can eventually commercialize) will cause the United States to lose to China.

In this paper, we argue instead that there is a better way to ensure artificial intelligence advances U.S. national security: public AI. By public AI, we mean two things: publicly-provided, -owned and -operated layers in the AI tech stack, such as cloud infrastructure, data, and model development; and public utility-style regulation of the private AI industry that fosters competition and prevents abuses of power. In the process, we show that relying on unregulated AI national champions[2]—an unbridled Silicon Valley—carries considerable risks for national security.

[1] Sam Altman, *Who Will Control The Future of AI?*, WASH. POST (July 5, 2024), https://www.washingtonpost.com/opinions/2024/07/25/sam-altman-ai-democracy-authoritarianism-future/.

[2] By unregulated, we do not mean literally unregulated. Obviously, standard American laws—workplace safety, tax, corporate governance, and other laws and regulations—apply. Rather, we mean regulations governing market structure. This is a critical distinction because the firms' status as national champions is about their dominance and market power.

The paper proceeds in four parts. In Part I, we discuss why AI matters for national security. Part II outlines what we mean by public AI—robust public options and capacity for aspects of the tech stack, and public-utility style regulation. Part III makes the case for how public AI will enhance national security, especially compared to a system of unregulated national champions. Part IV addresses a few additional criticisms. One caveat is worth noting: we do not address the ongoing debate over the national security risks and merits of closed versus open source AI foundation model development. Although we recognize the importance of that debate, we focus exclusively on the U.S. government's AI capacity and on public-utility style regulations.

I. Why AI Matters for National Security

There is a broad consensus within the bipartisan national security establishment that American national security requires the United States to remain on the cutting edge of AI innovation and applications.[3] The bipartisan National Security Commission on AI (NSCAI), which exemplifies this consensus, concluded in its final report in 2021:

> The pace of AI innovation is not flat; it is accelerating. If the United States does not act, it will likely lose its leadership position in AI to China in the next decade and become more vulnerable to a spectrum of AI-enabled threats from a host of state and non-state actors.... We know adversaries are determined to turn AI capabilities against us. We know a competitor is determined to surpass us in AI leadership. We know AI is accelerating breakthroughs in a wide array of fields. We know that whoever translates AI developments into applications first will have the advantage.[4]

There are three primary reasons for this geotechnological imperative. First is the critical role of AI in giving America the edge in its global competition with China.[5] This

[3] *See, e.g.,* NAT'L SEC. COMM'N ON A.I., FINAL REPORT (2021), https://reports.nscai.gov/final-report/ [hereinafter NSCAI REPORT]; Ashley Carnahan, *Former House China hawk warns Americans about the dangers of the CCP's growing technological dominance*, FOX NEWS (Sept. 24, 2024), https://www.foxnews.com/media/former-house-china-hawk-warns-americans-about-dangers-ccps-growing-technological-dominance (on former Republican congressman Mike Gallagher's views on the importance of AI for national security); Rishi Iyengar, *The Technocrat,* FOREIGN POL'Y (Aug 16, 2024), https://foreignpolicy.com/2024/08/16/gina-raimondo-us-china-tech-competition-chips-ai/ (on Democratic Commerce Secretary Gina Raimondo's views on the importance of AI for national security).

[4] NSCAI REPORT, *supra* note 3, at 19, 28.

[5] For a list of these arguments, and related ones, see *Tracking the US and China AI Arms Race,* AI NOW INST. (Apr. 11, 2023), https://ainowinstitute.org/publication/tracking-the-us-and-china-ai-arms-race.

competition is comprehensive and multifaceted. The two countries are vying for economic and military preeminence, for regional allies and diplomatic advantage, and for political and cultural influence across the globe. Which country's technologies enable military strength, become the platforms for global commerce, and shape politics and culture in the 21st century might be decisive in this competition. Even if AI becomes even half as transformative and integral to our lives as techno-optimists expect, the United States has an important national interest in leading in both AI innovation and safety, which, according to leading U.S. policymakers, go hand in hand.[6]

Vice President Kamala Harris, National Security Advisor Jake Sullivan, and the bipartisan NSCAI have all argued that staying on the cutting edge of AI that is rooted in democratic values with a privacy- and rights-protecting orientation is essential to defending democracy and America's global leadership.[7] Key to staying on the cutting edge, and therefore strengthening national security, is an active recognition of the technology's numerous downside risks and harms.[8] Many of the use cases for AI carry considerable risks to civil rights and civil liberties, as well as to human rights, democratic institutions, and competitive markets. The Biden Administration's Blueprint for an AI Bill of Rights and Executive Order on Artificial Intelligence recognized these realities, and exhorted efforts across the whole of government and society to address these risks so that we could realize AI's public benefits.[9] If the globally-dominant AI systems that emerge in the coming years do not uphold and further these values, AI's adoption may threaten the resilience of democracies around the world. Alternatively, developing a democracy-, privacy-, and rights-protecting AI could improve American democracy and national defense and offer an alternative model for other countries to emulate.

[6] *See, e.g.,* Tharin Pillay, *Time100 AI 2024: Elizabeth Kelly, Director, United States Artificial Intelligence Safety Institute*, TIME (Sept. 5, 2024), https://time.com/7012783/elizabeth-kelly/ ("'Our view is that safety enables trust, which enables adoption, which enables innovation,' Kelly says.").

[7] Andrew Macaskill and Martin Coulter, *US Vice President Harris calls for action on "full spectrum" of AI risks*, REUTERS (Nov. 1, 2023), https://www.reuters.com/technology/us-vice-president-harris-call-action-threats-ai-2023-11-01/; Patrick Tucker, *Sullivan: Data Privacy Key To AI Race Against China*, DEFENSE ONE (July 13, 2021), https://www.defenseone.com/technology/2021/07/sullivan-data-privacy-key-ai-race-against-china/183747/; *see generally* NSCAI REPORT, *supra* note 3.

[8] *See, e.g., Recognize Potential Harms and Risks*, NAT'L TELECOMM. & INFO. ADMIN. (Mar. 27, 2024), https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report/requisites-for-ai-accountability-areas-of-significant-commenter-agreement/recognize-potential-harms-and-risks.

[9] *See* Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023) [hereinafter "AI EO"].

Second, AI systems have already been used, are currently being used, and will only become more important to warfare, national defense, and homeland security. Whatever one thinks of the ongoing conflicts in Ukraine and Gaza, AI has played a significant role in both.[10] Senior military and defense leaders also believe that AI will play a critical role in military organization, deterrence, threat anticipation, and warfighting,[11] even as some observe that the U.S. military is not ready for this new era.[12] There is also little doubt that increasingly powerful AI with the ability to integrate vast quantities of data extremely quickly with heretofore unseen capacity for problem solving and predictive potential will become even more important for intelligence analysis and national security planning. For its part, the Biden Administration's EO directed a new national security memorandum to guide "the continued adoption of AI capabilities to advance the United States national security mission."[13]

Moreover, AI will have applications across federal agencies that support homeland security and resilience, from cybersecurity and critical infrastructure protection to counterterrorism to counternarcotics, from ensuring public health (including in future pandemics) to defending against foreign disinformation and election interference. Indeed, should advanced AI be used to attack or weaken America's economy, military, democracy, and critical infrastructure or those of its allies, the federal government, state governments and industry will almost certainly have to use even better AI capabilities to defend against, remediate, and counter these attacks.

[10] *See, e.g.,* Robin Fontes and Dr. Jorrit Kamminga, Ukraine A Living Lab for AI Warfare, NAT'L DEFENSE (Mar. 24, 2023), https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare (on the use of AI in the Russo-Ukraine War); Geoff Brumfiel, *Israel is Using an AI System to Find Targets in Gaza. Experts Say It's Just The Start*, NPR (Dec. 14, 2023), https://www.npr.org/2023/12/14/1218643254/israel-is-using-an-ai-system-to-find-targets-in-gaza-experts-say-its-just-the-st (on Israel's use of AI in Gaza).

[11] Brit McCandless Farmer*, AI In The Military: Gen. Milley On the Future of Warfare*, CBS NEWS (Oct. 8, 2023, https://www.cbsnews.com/news/artificial-intelligence-in-military-general-mark-milley-future-of-warfare-60-minutes/ (on General Mark Milley's view of the importance of AI and robotics to America's future military power); U.S. DEP'T OF DEFENSE, REMARKS BY DEPUTY SECRETARY OF DEFENSE KATHLEEN H. HICKS ON 'THE STATE OF AI IN THE DEPARTMENT OF DEFENSE' (AS DELIVERED) (2023), https://www.defense.gov/News/Speeches/Speech/Article/3578046/.

[12] *See, e.g.,* Raj M. Shah and Christopher M. Kirchhoff, The U.S. Military Is Not Ready for the New Era of Warfare, N. Y. Times (Sept. 13, 2024), https://www.nytimes.com/2024/09/13/opinion/ai-drones-robot-war-pentagon.html; REPORT OF THE COMMISSION ON THE NATIONAL DEFENSE STRATEGY (Sept. 2024), https://www.armed-services.senate.gov/imo/media/doc/nds_commission_final_report.pdf.

[13] Alexandra Kelley, *Memo on AI's National-Security Implications Heads for Biden's Desk*, DEFENSE ONE (July 26, 2024), https://www.defenseone.com/threats/2024/07/biden-receive-ai-national-security-memo-outlining-forbidden-uses-areas-innovation/398382/; AI EO, *supra* note 9.

Third is the remote but non-negligible concern about the potentially existential risks of AI. Some of the most prominent voices in AI, including CEOs of the leading AI labs, have repeatedly warned that increasingly powerful AI could pose either catastrophic and existential risks to humanity in the coming years.[14] (Of course, they continue to develop the technology toward Artificial General Intelligence (AGI) as quickly as possible, accelerating these potential risks.) There are wide ranging opinions on the probability, or even possibility, of such risks and so-called "emergent properties" for frontier AI. Nonetheless, taking these risks seriously means that the U.S. government should be at the cutting edge of AI safety research.

II. Public AI

To facilitate an AI future that supports American national security, the United States should embrace the public sector's role in building, developing, and governing artificial intelligence. We call this framework "public AI." Public AI would manifest in two ways: (1) developing publicly-funded, publicly-owned, and publicly-run AI tech stacks, that coexist alongside private ones; and (2) adopting public-utility style regulations to layers in the AI tech stack to ensure innovation, enhance competition, advance the national interest, protect democracy, and respect taxpayers.

A. Public Options for AI

By a public option for AI, we mean publicly-provided and publicly-run aspects of the AI tech stack – essentially the supply chain for AI.[15] The tech stack is comprised of four layers: hardware, cloud infrastructure, data and models, and applications. At the base of the supply chain is hardware, including photolithography equipment and graphical processing units (GPUs) or chips. Both of these hardware elements operate in monopoly or near-monopoly conditions, and are extremely expensive. This hardware is used to build cloud infrastructure, which provides the computing power needed at scale – and only a few companies in the world can pay the high capital costs required

[14] *See, e.g.*, Billy Perrigo, *AI Is as Risky as Pandemics and Nuclear War, Top CEOs Say, Urging Global Cooperation*, TIME (May 30, 2023), https://time.com/6283386/ai-risk-openai-deepmind-letter/; *Statement on AI Risk*, CENTER FOR AI SAFETY, https://www.safe.ai/work/statement-on-ai-risk (last visited Sept. 26, 2024).

[15] *See* Tejas Narechania and Ganesh Sitaraman, *An Antinomonpoly Approach to Governing Artificial Intelligence*, Yale L. & Pol'y Rev. 46-48 (forthcoming 2025), https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2023/10/06212048/Narechania-Sitaraman-Antimonopoly-AI-2023.10.6.pdf.pdf.

to build cloud infrastructure at scale using these GPUs. The next layer in the stack is data and models. Vast quantities of data are the raw material for AI to learn, and models work because of the data – they are trained on the data to learn and execute specific tasks. This process of training requires enormous amounts of compute power, at high cost. Only after models are developed are user-facing applications possible.[16]

A public option for AI would include more significant government investment to do the following: build more public data centers; host and train AI using public cloud services on publicly-owned and operated cloud infrastructure; organize public data for AI model development and bespoke national security and public interest applications; and hire significant AI human talent into the government.

This last element is critical: public capacity requires people. For many years, the federal government's approach has been to contract out such services. The downsides of this approach have since been well-documented: dependence on consulting firms that charge high rates for work of varying quality; high profile failures like the Affordable Care Act website rollout; and a sapping of governmental capacity more broadly.[17] Investing in people with technological expertise has the potential to create a virtuous cycle: a more affordable mission-driven staff would not only build public-interested AI systems for a wide variety of public- uses but could also evaluate private sector AI services more accurately and reduce the likelihood that government contracts will suffer from cost and quality problems.

Notably, the United States already has important nascent efforts at "public" AI. The National AI Research Resource (NAIRR) is a federal initiative currently in a pilot phase.[18] It aims to connect U.S. researchers and educators to computational, data, and training resources needed to "spur innovation, increase diversity of talent, improve capacity, and advance safe, secure, and trustworthy AI in research and society." The NAIRR, however, is small-scale in terms of the number of not-for-profit projects it can support. Problematically, the pilot program and larger concept are not truly public: it depends

[16] For a more thorough discussion of the AI tech stack, see *id.*, at 8-21.

[17] For discussions, see Ganesh Sitaraman and Ramsay Eyre, *Building Public Capacity on Artificial Intelligence*, VAND. POL'Y ACCELERATOR (2023), https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2023/10/09151836/VPA-AI-Capacity.10.9.23.pdf; MARIANA MAZZUCATO & ROSIE COLLINGTON, THE BIG CON: HOW THE CONSULTING INDUSTRY WEAKENS OUR BUSINESSES, INFANTILIZES OUR GOVERNMENTS AND WARPS OUR ECONOMIES (2023); JENNIFER PAHLKA, RECODING AMERICA: WHY GOVERNMENT IS FAILING IN THE DIGITAL AGE AND HOW WE CAN DO BETTER (2023).

[18] THE NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH RESOURCE (NAIRR) PILOT, https://nairrpilot.org/ (last visited Sept. 22, 2024).

on the private sector and the dominant AI firms to contribute compute and other resources for NAIRR researchers to use.[19] The legislation which first proposed the NAIRR is studiously unclear on whether compute infrastructure will be publicly or privately provided.[20]

The recently announced Department of Energy FASST AI initiative proposes to use DOE's data, workforce and supercomputers to drive AI advances for national security, scientific discovery, energy challenges, and AI safety expertise. The President's budget has requested $455 million for it.[21] Here, too, it seems that the DOE will rely on some private sector AI infrastructure and partnerships (including cloud, data centers, and likely software designers). Even if funding is appropriated for FASST, it is unclear whether the requested amount is enough to achieve the aims of the program, especially its national security mission, let alone a more expansive set of public interest missions. There is also DOD's Joint Common (AI) Platform (JCP), launched in March 2021 which provides services, capabilities, and resources to build AI models for

[19] Amba Kak, *The Problem With Public-Private Partnerships in AI*, FOREIGN POL'Y (Feb. 12, 2024), https://foreignpolicy.com/2024/02/12/ai-public-private-partnerships-task-force-nairr/.

[20] CREATE AI Act of 2023, S. 2714, 118th Cong. (1st Sess. 2023) ("The NAIRR shall offer resources that include, at a minimum, all of the following, subject to the availability of appropriations: (1) A mix of computational resources, including . . . (B) public cloud providers providing access to popular computational and storage services for NAIRR users[.]"). *Public* cloud, in this context, refers not only to public-sector compute infrastructure, but also to privately-owned cloud infrastructure-as-a-service available to a wide range of customers, as contrasted with *private* cloud, which refers to infrastructure available only to an organization's internal users. For a discussion of the history of the legislative proposal, see Kak, *supra* note 19.

[21] DEPT. OF ENERGY, FY 2025 BUDGET IN BRIEF: FY2025 CONGRESSIONAL JUSTIFICATION 3 (2024), https://www.energy.gov/sites/default/files/2024-03/doe-fy-2025-budget-in-brief-v2.pdf; *Frontiers in Artificial Intelligence for Science, Security and Technology (FASST)*, DEP'T OF ENERGY OFF. OF CRITICAL & EMERGING TECH., https://www.energy.gov/fasst (last visited Sept. 22, 2024); Alison Snyder, *DOE aims to move "FASST" on AI with sweeping new initiative*, AXIOS (May 7, 2024), https://www.axios.com/2024/05/07/artificial-intelligence-doe-faast. For more on funding projections for FASST, see Nyah Stewart, *Fueling Innovation: Insights Into Federal AI R&D Funding*, SPECIAL COMPETITIVE STUDIES PROJECT 13, fn 23 (Sept. 2024), https://www.scsp.ai/wp-content/uploads/2024/09/2.0_-AI-RD-White-Paper.pdf.

defense and military needs.[22] It too relies on private cloud and was developed and operated by a private contractor.[23]

NAIRR, FASST, and JCP are important steps in the right direction, but they ultimately fall short of building public AI capacity and are not sufficiently ambitious in either scale or scope. More robust federal investment in the infrastructure and human capacity for public AI is needed.

B. Public Governance of AI

The second, and complementary, effort is to apply public-utility style regulations to the monopolistic or oligopolistic private sector firms that dominate the AI stack. Such regulations have been a longstanding part of American law and public policy. The American tradition of public utility regulation recognized that in sectors that feature network effects, economies of scale, and are likely to be highly concentrated, regulation was necessary to, among other things, to prevent abuses of market power, enhance innovation, ensure competition, protect consumers, and guarantee the provision of essential services. For national security purposes, the most relevant regulatory tools in this tradition are structural separations, nondiscrimination rules, and restrictions on foreign ownership.

Structural separations ensure that providers of essential infrastructure do not also provide the services that use that infrastructure. For example, railroads were banned from also owning companies that provided goods that traveled on the railroads (like coal). The reason is obvious: the railroad would only serve its own vertically-integrated coal company or would charge prohibitive prices to competitors, thereby pushing them out of business. A competitive coal sector required preventing vertical integration with railroads. In the AI context, structural separations could be placed between chip makers, cloud providers, and model developers to ensure that these respective actors

[22] *Joint Common Foundation (JCF)*, CHIEF DIGIT. AND A.I. OFF., https://www.ai.mil/index.html (last visited Sept. 22, 2024) ("The Joint Common Foundation (JCF) is a secure cloud-based AI development and experimentation environment that delivers critical tools and capabilities to support the DoD's pursuit of an AI-ready force.").

[23] Jackson Barnett, *With $106M contract, JAIC takes major step building central AI platform for DOD*, FEDSCOOP (Aug. 13, 2020), https://fedscoop.com/jaic-ai-development-platform-dod-joint-common-foundation-deloitte/; Jackson Barnett, *Pentagon's Joint Common Foundation AI platform is up and running*, FEDSCOOP (Mar. 23, 2021), https://fedscoop.com/joint-common-foundation-ai-platform-launched/.

do not leverage their gatekeeping power in one market to dominate other actors in the AI stack – including America's military and federal, local, and state governments.

Nondiscrimination rules, or neutrality mandates, require that infrastructural providers serve all comers neutrally without favoritism or price discrimination. This approach ensures that users (whether businesses, government, or others) can access the essential services that they depend on to operate, and that the platforms cannot pick and choose which businesses live or die. Nondiscrimination rules ensure a level competitive playing field for entrepreneurs and non-profit, academic, or public sector customers to access critical resources. In the AI context, these rules would apply to chip makers, cloud providers and model developers.

Restrictions on foreign ownership, control, and investment in infrastructure industries have also been common – particularly when national security, critical public services, and resilience are at stake, as they are with AI. These rules can be designed in different ways but have historically included requirements that firms and directors be American citizens and that ownership be predominantly American. Regulations also govern export controls. In the AI and tech context, similar rules should be applied to AI providers across the stack, depending on the degree to which there are national security issues at stake in the given layer. Indeed, the Biden Administration is already taking actions along these lines with respect to China and could be even more circumspect about the partnerships between Silicon Valley and U.S. adversaries, competitors, and countries that do not share America's values and interests.[24]

Public-utility style regulations complement the expansion of public AI stacks and the U.S. government's AI capacity. The reason is that the United States needs a competitive and dynamic private AI industry for national security reasons. Without competition or regulation, an AI oligopoly is likely to box out innovative start-ups, lose their innovative edge, offer worse quality of service to government clients, and raise costs for the American taxpayer. Regulating market structure to prevent the abuses of monopoly and oligopoly power would also make it more viable for the federal government, and state and local governments, to use private contractors when necessary – without fear that doing so would undermine innovation, effectiveness, or resilience.

[24] Alexander Cornwell, *UAE seeks closer AI, tech ties in Biden talks as China interest stirs US concern*, REUTERS (Sept. 23, 2024), https://www.reuters.com/technology/uae-seeks-closer-ai-tech-ties-biden-talks-china-interest-stirs-us-concern-2024-09-23/.

III. How Public AI Enhances National Security

A more robust role for the public in developing and governing AI, combining high-capacity public options and traditional, American public-utility style regulations would strengthen U.S. national security. In particular, this approach is superior to a system in which the United States relies only on unregulated national champions for AI. There are four reasons for why public AI is better for national security than exclusive dependence on private tech companies.

A. Innovation and Independence for National Security

First and foremost, public AI would bolster innovation. As Mariana Mazzucato has shown, the federal government has been an engine of innovation – and particularly technological innovation - throughout its history.[25] Research and development programs, national missions and industrial policies, and other publicly-resourced and often publicly-run programs have led to considerable breakthroughs. We should expect that well-resourced public AI tech stacks and human talent will facilitate national security and other public-interested innovations as well. Unlike AI developed by Silicon Valley, public AI would be democratically accountable and is likely to have greater oversight from Congress, courts, and the media. Public AI's innovations would be directed at national needs and missions, including addressing public problems, solving national security challenges, and importantly, improving AI safety itself.

Public AI is also superior to relying solely on unregulated private tech firms, especially in concentrated markets. It is textbook economics that firms facing little competition and no regulation to discipline them will both abuse their power and fail to innovate. In fact, they will even actively stifle innovation by other firms to maintain market dominance.[26] We have already seen precisely these dynamics in the tech sector.[27] Big

[25] *See generally* MARIANA MAZZUCATO, THE ENTREPRENEURIAL STATE: DEBUNKING PRIVATE VS. PUBLIC SECTOR MYTHS (2013); MARIANA MAZZUCATO, THE MISSION ECONOMY: A MOONSHOT GUIDE TO CHANGING CAPITALISM (2021).

[26] For a recent academic discussion of the mechanisms by which dominant firms reduce disruptive innovation, see Mark A. Lemley and Matthew T. Wansley, *Coopting Disruption* (forthcoming 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4713845 (discussing, among other things, acquisitions).

[27] *See, e.g.* Lina Khan, Amazon's Antitrust Paradox, 126 YALE L.J. 564 (2017); Lina Khan, The Separation of Platforms and Commerce, 119 COLUM. L. REV. 973 (2019); Investigation of Competition in Digital Markets:

tech platforms have been sued for a wide range of abuses of power–including in ways that destroy innovation. Indeed, lawsuits on precisely these grounds are currently pending against Google and Amazon.[28] In light of the last two decades of tech history, which have culminated in a flood of antitrust cases, we should expect these firms to continue pursuing anticompetitive actions that undermine innovation as they move into the AI space. Robust, independent public AI capacity also allows for more bespoke experimentation and innovation tailored to the U.S. government's (and the American people's) needs, unencumbered by the drive to monetize innovations.

Public AI also gives the federal government independence from market actors with countervailing or conflicted interests. Consider Elon Musk's control of Starlink for example.[29] Whatever one thinks of Musk's political views or the war in Ukraine, should one person–or one firm–be able to undermine U.S. government policy with respect to a major conflict simply because they want to?[30] Reliance solely on unregulated national champions makes the U.S. government dependent on a small number of firms–and even on particular individuals. This is a tactical and strategic national security risk because one person or firm holds considerable power over the government. In the contracting context, this danger often manifests as the "lock in" problem. Sole source contractors can demand concessions, charge higher prices, and operate in private markets with relative impunity because the government has no alternatives. There is

H. Comm. On The Judiciary, 117th Congress (2022), https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf?stream=top; Charles Duhigg, *The Case Against Google,* N.Y. TIMES MAG. (Feb. 20, 2018), https://www.nytimes.com/2018/02/20/magazine/the-case-against-google.html; Dana Mattoli, *How Amazon Wins: By Steamrolling Rivals and Partners*, WALL ST. J. (Dec. 22, 2020), https://www.wsj.com/articles/amazon-competition-shopify-wayfair-allbirds-antitrust-11608235127.

[28] *See, e.g.,* United States v. Google LLC, 687 F.Supp.3d 48 (2024); Fed. Trade Comm'n v. Amazon.com, Inc., No. 2:23-cv-01495 (W.D. Wash. filed Sept. 26, 2023); Press Release, OFF. OF PUB. AFFS., U.S. DEP'T OF JUST., Justice Department Sues Google for Monopolizing Digital Advertising Technologies (Jan. 24, 2023), https://www.justice.gov/opa/pr/justice-department-sues-google-monopolizing-digital-advertising-technologies; Press Release, OFF. OF PUB. AFFS., U.S. DEP'T OF JUST., Justice Department Sues Monopolist Google For Violating Antitrust Laws, (Oct. 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws; *FTC Sues Amazon for Illegally Maintaining Monopoly Power*, FED. TRADE COMM'N. (Sept. 26, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power.

[29] *See* Henry Farrell and Abraham Newman, *What Happens When Tech Bros Run National Security*, TIME (Sept. 20, 2023), https://time.com/6315670/big-tech-national-security/.

[30] Victoria Kim, *Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack,* N.Y. TIMES (Sept. 8, 2023), https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html.

also the quite real prospect of a contractor withholding critical products and services if the firm's leadership has a policy or political difference with the U.S. government.

Dependence is itself a national security danger. As the recent Crowdstrike outage and hack of Microsoft's government clients attest, dependence by government or critical infrastructure entities (such as utilities or airlines) on sole source providers for foundational operations services creates national security risk.[31] This is not an AI-specific problem, of course, but as AI becomes increasingly central to U.S. national security, the dangers of government dependence on one or an oligopoly of AI firms grow. The U.S. government must anticipate and studiously avoid these risks.

Public AI offers a remedy to some of the problems of dependence. Public AI stacks create an independent option for government, one free from conflicts of interests or the whims of powerful private citizens. It ensures that national security goals cannot be dictated or determined by private actors. Even if the public option is limited to public uses, and not commercially available, its very existence will also inject greater competition into the AI ecosystem because the government could in-source activities if market offerings are inadequate or suboptimal. When government does need to leverage the private sector, a robust, independent public AI capacity will improve its ability to effectively partner with industry to advance the national interest. Importantly, the public AI stack could also focus on different, and public-spirited, goals for research, development, innovation and service provision.

Pro-competition regulations such as structural separations and non-discrimination rules will also enhance innovation – by helping ensure that the whole AI stack has accessible and competitive markets. They also prevent abuses of power, like discriminatory pricing for infrastructural services. This expands the pool of contractors with whom the government can work, so the federal government has more choices to support military, defense, intelligence and homeland security missions – and no single actor can dictate terms. In short, these regulations would help keep the AI ecosystem healthy for the situations in which contracting out is necessary.

[31] Rachyl Jones, *CrowdStrike ex-employees: 'Quality control was not part of our process'*, SEMAFOR (Sept. 12, 2024), https://www.semafor.com/article/09/12/2024/ex-crowdstrike-employees-detail-rising-technical-errors-before-july-outage; Renee Dudley and Doris Burke, *Microsoft Chose Profit Over Security and Left U.S. Government Vulnerable to Russian Hack, Whistleblower Says*, NEXTGOV (June 13, 2024), https://www.nextgov.com/cybersecurity/2024/06/microsoft-chose-profit-over-security-and-left-us-government-vulnerable-russian-hack-whistleblower-says/397349/.

B. Public AI for Public Goods

A well-resourced public option for AI would invariably address different questions than private firms. AI companies are primarily interested in making money and they have made significant investments on which their shareholders will demand a return. As a result, in areas where public goods – including national and homeland security missions – are at issue the market will likely under-invest unless lucrative government contracts are available. The tech platform example is instructive: countless hours and billions of dollars have been spent optimizing what videos and advertisements people should see. Far less effort in our age of technological progress has gone toward improving veterans benefits or social welfare programs – because that's not where the money is.

One response, of course, is that there will be lucrative government contracts available for certain needs, so firms will enter the market to bid and win that guaranteed revenue. Indeed, Microsoft, Amazon, Palatir, and Anduril and other tech companies are already operating in the defense and national security space. But relying on Big Tech and AI juggernauts through defense contracting has significant downsides for the public. Consider traditional defense contracting as an analogy. No one today thinks that defense contracting is optimal, including DOD leadership.[32] Cost-overruns and delivery delays are standard.[33] Quality of the output is sometimes a problem. For decades, even when contracts with firms are over-budget, delayed, and the systems don't work, the government continues to make deals with those same firms because there is little competition and high sunk costs.[34] Despite efforts by DOD to reform this process for new technologies, contracting out for various AI products and services might simply replicate a system that isn't working.[35] Even if the system does not replicate all of these pathologies, once national security needs are identified,

[32] *See, e.g.*, Joe Gould, *Kathleen Hicks warns of 'substantial decline' in defense-industrial base competition*, DEFENSE NEWS (Apr. 12, 2022), https://www.defensenews.com/pentagon/2022/04/12/kathleen-hicks-warns-of-substantial-decline-in-defense-industrial-base-competition/.

[33] *See, e.g.*, Rose L. Thayer, *Delays in military construction have doubled in last 5 years often adding millions of dollars to the cost, watchdog finds*, STARS & STRIPES (Sept. 16, 2024), https://www.stripes.com/theaters/us/2024-09-16/military-construction-delays-15199919.html.

[34] *See generally* DEP'T OF DEFENSE, STATE OF COMPETITION WITHIN THE DEFENSE INDUSTRIAL BASE (2022), https://media.defense.gov/2022/Feb/15/2002939087/-1/-1/1/STATE-OF-COMPETITION-WITHIN-THE-DEFENSE-INDUSTRIAL-BASE.PDF.

[35] For a reputable analysis of consolidation in the defense industrial base and its consequences for American military readiness, see generally COMMISSION ON THE NATIONAL DEFENSE STRATEGY, FINAL REPORT (2024), https://www.armed-services.senate.gov/imo/media/doc/nds_commission_final_report.pdf.

contracting to private actors still takes a considerable amount of time compared to in-house development and delivery of solutions.

Public AI would ensure more attention to public goods that do not have a (demonstrable) return on investment. One can imagine researchers and developers using public AI resources to develop and deploy AI solutions to address thorny problems of poverty and food insecurity, climate change, and disease – and without the imperative to commercialize those solutions or achieve a return on the investment of time and money. Indeed, the government will not have to pay for the added costs of the profits that shareholders demand. Still, to the extent that contracting out is needed, public regulation will help ensure that the ecosystem of firms remains broad and innovative. If private companies understand that the government has the ability to develop national and homeland security solutions in-house, they would have to be more competitive in their pricing and more sensitive to delivering on time and on budget.

Public AI will thus help build and enhance state capacity to address public problems. As Mariana Mazzucato and Rosie Collington have argued, reliance on outsourcing to contractors and consultants saps the government of knowledge, talented people, and focus on public problems.[36] Building this capacity is important: agencies with technology experts will better understand what capabilities are needed and appropriate than those who outsource their capacity to think about and use technology. Moreover, having serious in-house AI expertise and capacity will improve federal agencies' capacity to evaluate private contractors' AI proposals and products, and in turn, ensure that the government gets the products and services it needs at a fair price. This is one reason why experts have recommended building up federal tech capacity and personnel across agencies.[37]

C. Advancing Safe and Democratic AI

AI should be built in a way that is safe for the public, rights-protecting and democracy-enhancing. This is important for America's long-term security. Most directly, if AI is developed in ways that are not safe, rights-protecting, and democracy-enhancing, its use risks fostering domestic strife and inequality and undermining national stability

[36] *See* MAZZUCATO & COLLINGTON, *supra* note 17.

[37] *See generally* PAHLKA, *supra* note 17; Sitaraman and Eyre, *supra* note 17.

and resilience. More broadly, to the extent that other countries are comparing the United States and China in this new era of competition, offering an appealing path for adopting and using AI and other technologies should increase America's geopolitical influence. In short, developing and deploying effective AI that safeguards – and ideally strengthens – democracy and rights will ensure that the United States preserves Americans' civil rights and republican institutions, and it would serve as a model and a baseline for others around the world, thereby strengthening U.S. global leadership.

Relying on the Big Tech and the commercial AI industry to provide safe, rights-protecting, and democracy-enhancing AI is naive given the experience with Silicon Valley over the last 30 years. At best, big tech companies have a mixed record when it comes to public safety and welfare and democratic practices. The list of inadequate safeguards, design failures, lags in remediation, and problematic intentional actions is long: the lack of protection of children on social media; the vast collection of data and disregard for privacy; the platform-enabled hacking and influence on American elections, including by selling and sharing data; and problematic labor practices that support training data production and content moderation.[38] Some frontier AI companies have already been sued for training their models using massive amounts of copyrighted materials without permission or payment.[39] Add to this the fact that the big tech companies that operate globally comply with the conditions placed on them by foreign governments – including authoritarian ones – and it is not clear that these firms will always champion civil rights and democracy. It is possible they could become the handmaidens of authoritarianism, when and where market access requires it.

Of course, the federal government is not perfect either, especially in the national security context. The U.S. government has undertaken its fair share of undemocratic

[38] *See, e.g.,* Shannon Bond and Bobby Allyn, *Whistleblower tells Congress that Facebook products harm kids and democracy*, NPR (Oct. 15, 2021), https://www.npr.org/2021/10/05/1043207218/whistleblower-to-congress-facebook-products-harm-children-and-weaken-democracy; SOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019); Billy Perrigo, *OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic*, TIME (Jan. 18, 2023), https://time.com/6247678/openai-chatgpt-kenya-workers/; Niamh Rowe, '*It's destroyed me completely*'*: Kenyan moderators decry toll of training of AI models*, THE GUARDIAN (Aug. 2, 2023), https://www.theguardian.com/technology/2023/aug/02/ai-chatbot-training-human-toll-content-moderator-meta-openai.

[39] Alexandra Alter and Elizabeth A. Harris, *Franzen, Grisham and Other Prominent Authors Sue OpenAI*, N. Y. TIMES (Sept. 20, 2023), https://www.nytimes.com/2023/09/20/books/authors-openai-lawsuit-chatgpt-copyright.html; Jordan Novet, *Eight newspaper publishers sue Microsoft and OpenAI over copyright infringement*, CNBC (Apr. 30, 2024), https://www.cnbc.com/2024/04/30/eight-newspaper-publishers-sue-openai-over-copyright-infringement.html?msockid=3e8b7a20b5a369613cc06917b4cc68ec.

and rights-abusing actions from domestic surveillance of civil rights leaders to bulk data collection. For this reason alone, public AI efforts should be accompanied by strict privacy rules and independent oversight to ensure Americans' rights. But in creating a public option for AI, lawmakers have the opportunity to advance, rather than diminish, democratic values and establish layers of oversight and transparency, which importantly - and unlike private companies - are democratically accountable.

D. The Public Role in High-Risk Activities

A fourth national security reason for public AI speaks to the risks of the technology and the imperative to ensure AI safety keeps pace with frontier AI development. AI safety is a public good, and despite interest in the topic, the private sector dramatically under-invests in it.[40] Some firms also seem to treat AI safety as an afterthought, which has led to a number of alternative firms created by disaffected and worried former employees.[41] Leading figures in the AI sector, including the heads of frontier AI companies, have warned that generative AI models pose catastrophic and potentially existential risks to humanity – including the risk of "large-scale destruction" within a few years.[42] Some have even declared that the future generative AI models will be so powerful and risk-laden that they should not be in private hands.[43] There are wide-ranging opinions on the probability, or even possibility, of such risks and so-called "emergent properties" for frontier AI. But if these risks are taken seriously, as some

[40] Reed Albergotti, *Despite the AI safety hype, a new study finds little research on the topic*, SEMAFOR (Apr. 3, 2024), https://www.semafor.com/article/04/03/2024/despite-the-ai-safety-hype-a-new-study-finds-little-research-on-the-topic. For an overview of the field of AI safety and a Biden Administration effort to advance it, see *U.S. Artificial Intelligence Safety Institute*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/aisi (last visited Sept. 22, 2024).

[41] Two examples are Dario Amodei's departure from OpenAI to found Anthropic, over reported disagreements about AI safety; and former OpenAI executive Ilya Stutskever's new firm, Safe Superintelligence. *See* Sharon Goldman, *As Anthropic seeks billions to take on OpenAI, 'industrial capture' is nigh. Or is it?*, VENTUREBEAT (Apr. 7, 2023), https://venturebeat.com/ai/as-anthropic-seeks-billions-to-take-on-openai-industrial-capture-is-nigh-or-is-it/; Stephen Sorace, *OpenAI co-founder raises $1B for startup with single goal: safe superintelligence*, FOX BUSINESS (Sept. 9, 2024), https://www.foxbusiness.com/technology/openai-co-founder-raises-1b-startup-single-goal-safe-superintelligence.

[42] *Oversight of A.I.: Principles for Regulation: Hearing Before the S. Comm. on the Judiciary, Subcomm. On Privacy, Technology, and the Law*, 118th Cong. 2 (2023) (statement of Daro Amodei Ph.D, Co-Founder and CEO, Anthropic), https://www.judiciary.senate.gov/imo/media/doc/2023-07-26_-_testimony_-_amodei.pdf.

[43] *See* The Ezra Klein Show, *What if Dario Amodei Is Right About A.I.?*, N. Y. TIMES (Apr. 12, 2024), https://www.nytimes.com/2024/04/12/opinion/ezra-klein-podcast-dario-amodei.html.

democratic governments and engineers close to the most capable AI systems do,[44] then the U.S. government should be at the cutting edge of AI safety research. And to conduct cutting-edge AI safety research, the federal government needs its own AI capabilities on which public employees and outside independent non-profit researchers can build frontier models and conduct safety testing.

Moreover, if existential risks or emergent properties do materialize, it would likely be better for the first people to encounter and engage with such models to be public sector AI developers and national security professionals, who can be held publicly accountable, rather than corporate engineers and executives with primarily economic incentives.[45] There are three reasons for this. First, the government would most likely encounter and engage with any so-called AI "superintelligence" in a closed, classified facility rather than a more open corporate environment. This could help control and contain such a system. Second, corporate incentives will likely push in the direction of release without sufficient testing or controls. Silicon Valley and the larger tech industry have often adopted a "move fast and break things" approach that involves releasing products before fully developing them and considering their social implications.[46] When it comes to more powerful and capable AI models with greater potential for catastrophic and existential risk, there are self-evidently serious downsides to this approach. Third, and relatedly, the government has decades of experience (and is generally quite good at) maintaining security for extremely dangerous materials and sensitive information – from nuclear and cyber weapons to disease samples and state secrets. Indeed, this is one reason why these activities are either publicly run and publicly managed capabilities or are highly regulated.

IV. Addressing the Critics

Critics of public AI might raise a variety of concerns. First is that a regime of American AI national champions are our best hope to protect U.S. national security and out-compete China, and that anything that might impede them weakens the U.S. position

[44] *See, e.g.,* AI SAFETY SUMMIT, THE BLETCHLEY DECLARATION BY COUNTRIES ATTENDING THE AI SAFETY SUMMIT, 1-2 NOVEMBER 2023 (2023), https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration (an agreement on AI safety signed by 28 countries) [hereinafter BLETCHLEY DECLARATION].

[45] Public accountability would likely move through multiple mechanisms, including political appointees managing risks to the president, congressional oversight, and media scrutiny.

[46] *See, e.g.*, JONATHAN TAPLIN, MOVE FAST AND BREAK THINGS: HOW FACEBOOK, GOOGLE, AND AMAZON CORNERED CULTURE AND UNDERMINED DEMOCRACY (2017).

in this global competition. This concern is often raised in national security conversations. Mark Zuckerberg, for example, has observed that applying the antitrust laws and breaking up the American tech giants will simply mean that Chinese tech giants predominate.[47] Former Google Chief Eric Schmidt, who also co-chaired the NSCAI, has said he prefers industry self-regulation to government regulation of AI,[48] and regularly focuses on national security arguments. "China's not busy stopping things because of regulation," he has observed.[49] Some national security experts have similar views. One commentator, for example, holds that "regulation [including privacy regulations and anti-monopoly rules] should not be done in a way that kills U.S. innovation. . . . There is no evidence that the very strong U.S. innovation system is hampered by monopolies. . . . Breaking up big tech and hoping that increased competition will compensate is not an experiment to try in the middle of an intense and growing conflict with China."[50]

We have already discussed many of the downsides to monopolies and oligopolies, but these assertions rely on two erroneous assumptions: 1) that monopoly or oligopoly is better at innovation than a regulated, competitive ecosystem, and 2) that American companies always act in the national interest. On the former, proponents of big tech sometimes cite AT&T's monopoly and Bell Labs as an example.[51] This example, however, misses the critical context that AT&T was highly-regulated under telecommunications laws to ensure it met public service mandates at regulated rates,

[47] *See, e.g.*, Kurt Wagner, *Mark Zuckerberg says breaking up Facebook would pave the way for China's tech companies to dominate*, VOX (July 18, 2018), https://www.vox.com/2018/7/18/17584482/mark-zuckerberg-china-antitrust-breakup-artificial-intelligence; Nitasha Tiku, *Big Tech: Breaking Us Up Will Only Help China*, WIRED (May 23, 2019), https://www.wired.com/story/big-tech-breaking-will-only-help-china/.

[48] *See, e.g.*, Christaan Hetzner, *Former Google CEO Eric Schmidt tells government to leave A.I. regulation to Big Tech*, FORTUNE (May 15, 2023), https://fortune.com/2023/05/15/former-google-ceo-eric-schmidt-tells-government-to-leave-regulation-of-ai-to-big-tech-openai-chatgpt-bardai-midjourney/; @MeetThePress, X (May 24, 2023, 11:03 AM), https://twitter.com/MeetThePress/status/1657778656867909633 ("Former Google CEO @ericschmidt tells #MTP Reports the companies developing AI should be the ones to establish industry guardrails — not policy makers.").

[49] *A Global Perspective on AI With Eric Schmidt*, SCALE (Oct. 6, 2021), https://exchange.scale.com/public/videos/a-global-perspective-on-ai-with-eric-schmidt?utm_campaign=202112-transformx-youtube&utm_content=eric-schmidt-exchange-video-link&utm_funnel=awareness&utm_medium=organic-social&utm_source=youtube.

[50] James Andrew Lewis, *Tech Regulation Can Harm National Security*, CTR. FOR STRATEGIC & INT'L STUDIES (Nov. 28, 2022), https://www.csis.org/analysis/tech-regulation-can-harm-national-security.

[51] *See, e.g.*, Robert D. Atkinson, *America Needs Big Tech to Beat Big China*, INFO. TECH. & INNOVATION FOUND. (May 10, 2024), https://itif.org/publications/2024/05/10/america-needs-big-tech-to-beat-big-china/.

and that regulated profits enabled AT&T to support its innovative Bell Labs division.[52] In other words, it was *regulated*–not unregulated–monopoly that ensured innovation while simultaneously limiting the worst abuses of power.[53]

On the latter, the problem is that, notwithstanding the rhetoric of "tech patriotism"[54] or "patriotic capital,"[55] tech companies seek to maximize profits for their shareholders. But the profit motive does not necessarily overlap with the United States's national security interests or with the public interest.[56] Indeed, maximizing shareholder profits might require taking actions that are at odds with or even undermine U.S. national interests. That is why, for example, we have stringent export and arms control regulations that scrutinize weapons and tech transfers to certain countries and make some of them illegal.

Arguments about tech patriotism in the AI race with China are particularly questionable given that most of the big tech companies operate in China, are dependent on China for production of their hardware, or have consistently attempted to get into Chinese markets (and simply been thwarted by Chinese officials).[57] We have already seen evidence, or at least the concerning appearance, of conflicts of interest in which AI investors and developer companies maintain significant financial ties to and AI

[52] For a discussion of antimonopoly telecommunications regulation, see, *e.g.*, MORGAN RICKS, GANESH SITARAMAN, SHELLEY WELTON & LEV MENAND, NETWORKS, PLATFORMS, & UTILITIES: LAW & POLICY 319-392 (1st ed. 2022). On the amazing innovations of Bell Labs, SEE JON GERTNER, THE IDEA FACTORY: BELL LABS AND THE GREAT AGE OF AMERICAN INNOVATION (2012).

[53] Others argue that regulated monopoly was not as innovative as competition and suggest that horizontal break-ups are the preferred remedy. See, *e.g.*, Tim Wu, *What Should We Do About Google?*, N.Y. TIMES, Aug. 13, 2024, https://www.nytimes.com/2024/08/13/opinion/google-antitrust-remedy.html.

[54] *See* Cameron Costa, *How Palantir's tech-based patriotism and politics grew into a multi-billion dollar company*, CNBC (Oct. 13, 2022), https://www.cnbc.com/2022/10/13/how-palantirs-tech-patriotism-became-a-multi-billion-dollar-idea.html.

[55] *See* Heather Somerville, *As Silicon Valley Pivots to Patriotic Capital, China Ties Linger*, WALL ST. J. (May 12, 2024), https://www.wsj.com/finance/investing/as-silicon-valley-pivots-to-patriotic-capital-china-ties-linger-7030bf93.

[56] For one account, focused on manufacturing and applied research, see David Adler, *The American Way of Innovation and Its Deficiencies*, AM. AFFS. (2018), https://americanaffairsjournal.org/2018/05/the-american-way-of-innovation-and-its-deficiencies/.

[57] *See, e.g.*, Cheang Ming, *Google is blocked in China, but that's not stopping it from opening an A.I. center there*, CNBC (Dec. 13, 2017), https://www.cnbc.com/2017/12/13/alphabets-google-opens-china-ai-centre.html; Jack Nicas, Raymond Zhong, & Daisuke Wakabayashi, *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China*, N.Y. TIMES (May 17, 2021), https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html; *Amazon Web Services in China*, AMAZON, https://www.amazonaws.cn/en/about-aws/china/ (last visited Sept. 26, 2024).

investments in countries that are not exactly trustworthy US allies, such as China and the Gulf states.[58] It is not unrealistic to worry that such commercial ties to adversarial or diplomatically transactional countries could, if enough money or market share was at stake, undermine or at least complicate American firms' services to the U.S. government. Moreover, as we have recently seen in the context of the debate over banning TikTok, American private actors with significant economic stakes abroad can (and do) advocate for foreign interests in Washington.[59]

This is not in any way to charge these firms or their leaders with malign intentions. Rather, it is simply to say that profit seekers are likely to argue for policies that benefit their shareholders, not the American public, when these two sets of interests are at odds. Nor does this not mean that national security requires autarky. But it does enhance the case for public AI, which will reduce the government's dependence on tech companies that might have mixed motives, and for public-interest regulation, which will ensure a competitive domestic marketplace.

The second line of critique focuses on the challenges of developing public AI. Critics might charge that building robust, fully public AI tech stacks would be too expensive; that the federal government cannot build, hire or innovate fast enough to outpace China or American companies in AI; and that doing so would be redundant given existing private sector AI infrastructure and leadership.

We believe this critique misses the point and ignores American history. First, the sprint to build public AI would complement – not prevent, preclude, or crowd out – private AI infrastructure and investment. It would coexist with the private sector and address national security challenges and public goods, such as AI safety, in which the private sector under-invests. It would also ensure a dedicated, resilient, and uncompromised AI capacity that would meaningfully strengthen national security and advance public interest AI development, increase competitiveness (and lower the cost) of AI in the domestic market. Third, from the Manhattan Project to the Apollo program to the Internet to Operation Warpspeed, the U.S. Government has historically been a

[58] Courtney Degen, *House report says U.S. venture capital firms funded Chinese military interests*, PENSIONS & INVESTMENTS (Feb. 9, 2024), https://www.pionline.com/venture-capital/house-report-says-us-venture-capital-firms-funded-chinese-military-interests; Kimberley Kao, *U.S. Lawmakers Seek Probe of Microsoft's $1.5B Deal With Abu Dhabi AI Firm*, WALL ST. J. (July 12, 2024), https://www.wsj.com/tech/u-s-lawmakers-seek-probe-of-microsofts-1-5b-deal-with-abu-dhabi-ai-firm-1a1d35e3.

[59] *See, e.g.*, Clint Rainey, *Meet Jeff Yass, the billionaire ByteDance investor donating to Republicans who flipped against the TikTok ban*, FAST COMPANY (Mar. 14, 2024), https://www.fastcompany.com/91058467/who-is-jeff-yass-billionaire-donating-to-republicans-who-flipped-on-bytedance-tiktok-ban.

transformational innovator and enabler of public-interested technological innovation where there is an urgent and compelling national interest.[60] Finally, to the extent that building public AI would require transforming government – by hiring many new people with technological experience and expertise and increasing state capacity for public activities – this is a feature, not a bug. For too long, the government's capacity to act, and especially to act on technology, has been underdeveloped, slow, and outsourced. Building up capacity is itself an essential mission on its own terms, for reasons of both national security and good government.

Conclusion

America needs a dependable, resilient, and public-interested approach to AI that can harness and advance AI to safeguard our national security, compete effectively and sustainably with China, and benefit the American people in their daily lives. Our current, largely unregulated ecosystem of one GPU manufacturer, three Big Tech cloud providers, and a handful of AI labs at or affiliated with Big Tech companies will not provide the AI that the United States needs to safeguard national security and serve the public. Policymakers should redouble their attention on the public's role in developing, operating, and governing AI. Building public AI tech stacks and adopting public-utility style regulations for the layers of the private AI tech stack will ensure a competitive, innovative, reliable, and publicly accountable AI ecosystem, and ensure that AI advances U.S. national security and the public interest.

[60] On the latter point, consider nuclear power, the space program, and the Internet as just a few examples.