APRIL 2025

Future-Proofing U.S. Technology: Strategic Priorities Amid Chinese Tech Advancement

Edited by Kelsey Quinn & Eric Omorogieva

NEW LINES INSTITUTE
FOR STRATEGY AND POLICY

Future-Proofing U.S. Technology: Strategic Priorities Amid Chinese Tech Advancement

Contents

The views expressed in this report are those of the authors and not an official policy or position of the New Lines Institute.

Our mission is to provoke principled and transformative leadership based on peace and security, global communities, character, stewardship, and development.

Our purpose is to shape U.S. foreign policy based on a deep understanding of regional geopolitics and the value systems of those regions.

COVER: An intelligent humanoid robot works at the information desk of Zhongguancun International Innovation Center, the venue for the 2025 Zhongguancun Forum Annual Conference, on March 21, 2025, in Beijing, China. (VCG via Getty Images)

Foreword

A Strategic Approach to Geopolitical Rivalry with China

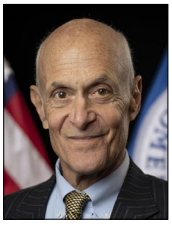
The global order is confronting a tectonic shift in the balance of power. After years in which the West enjoyed primacy in economic and technological innovation, competition has tightened. In particular, the Chinese now pose a profound challenge for influence and even dominance in these areas. A shift in the balance of power in these respects will raise profound concerns about our economic security and even our military and national security.

This changing landscape is the product of a number of developments. First, China's fusion of civil and military investment in technology development, coupled with the exploitation of espionage and intellectual property theft, have turbocharged that nation's development and exploitation of new inventions. Second, China has made overseas investments that have allowed broader access to critical minerals and resources that are prerequisite to building these new technologies. Third, the deployment of Chinese-owned or -controlled communications infrastructure around the world — including the West — has given China a powerful capability to influence or disrupt the economic and military capabilities of other nations.

For years China has understood that investment in, acquisition of, and influence over technologies that are economically critical will produce strategic advantage over other nations' security. During much of that time, the West treated national security as simply military capability, and economic innovation and investment as a separate matter for the free market.

Fortunately, Western thinkers have more recently understood the interdependency of economic capacity, supply chain robustness, technology innovation, and even climate change mitigation as elements of national security. Government investment and incentives for developing these areas are critical to ensure our freedoms and prosperity are secure. A strategic, all-hands-on-deck approach by democracies to developing new technologies is particularly important at this time, when breakthroughs in the fields of cyberspace, quantum mechanics, and artificial intelligence may bring revolutionary change to the way we live. In the right hands, these changes may make life safer and better; if controlled by geopolitical rivals, the reverse may happen.

The New Lines Institute compendium sets out a path forward to launch policies that take a comprehensive and strategic approach to advancing critical technologies in the West. As we compete with China for global influence in the coming decades, we must make sure that when our rivals play Go and chess, we are not simply playing checkers.



Hon. Michael Chertoff
United States Secretary of Homeland Security (2005-2009)

Introduction: Tech Sovereignty and Security

Edited by Kelsey Quinn & Eric Omorogieva

In an era defined by rapid technological advancement, the United States faces an unprecedented strategic challenge: maintaining its technological edge in the face of China's accelerating capabilities. This is not merely a competition for economic prosperity but a contest that will fundamentally alter global security, governance structures, and the values embedded in technologies that will shape tomorrow's world. As China pursues increasing technological self-sufficiency and primacy through its dual-circulation strategy and military-civil fusion, the United States must respond with policies that both protect its innovations and accelerate its development.

The technological rivalry between the United States and China transcends traditional geopolitical competition. It represents a systemic challenge that cuts across economic, security, and diplomatic domains. From artificial intelligence to quantum computing, from cybersecurity to critical resource supply chains, this competition demands a comprehensive, strategic response that harnesses America's innovative capacity while protecting its critical technologies from exploitation.

This compendium, "Future-Proofing U.S. Technology: Strategic Priorities Amid Chinese Tech Advancement," brings together diverse expertise to address this multifaceted challenge. The reports presented here examine critical technological domains where targeted policy action is needed to maintain U.S. strategic advantage. Each analysis offers concrete, actionable recommendations designed to enhance American competitiveness while countering China's advancing capabilities. Collectively, these analyses form a strategic roadmap for policymakers, industry leaders, and defense planners seeking to navigate the complex terrain of technological competition with China. They represent not just a warning about potential vulnerabilities but also a positive vision for how the United States can leverage its strengths to maintain technological leadership in the decades ahead.

"Strategic Implications of Alternative Payment Methods in a China-Taiwan Confrontation" examines how the People's Republic of China could use alternative payment systems to mitigate economic sanctions and reduce reliance on the U.S. dollar in a potential conflict over Taiwan. China's efforts to de-dollarize, particularly through partnerships with BRICS nations, signal a broader strategy with both economic and military implications. Currently, the United States lacks an action plan to counter these rising risks. This report highlights the need for proactive measures such as exploring stablecoins and leveraging sanctions as deterrents to reinforce U.S. economic influence and dollar hegemony.

In a world where artificial intelligence is increasingly shaped by geopolitics and power struggles, "Culture as a Tool for Trustworthy AI" explores how these forces influence the foundation of trust in AI systems. Currently, China offers not only the digital infrastructure needed for AI technologies but also an increasingly sophisticated variety of tools upon which future applications and large language models might be built, jeopardizing U.S. leadership in the sector. The piece delves into the intersection of culture, governance, and technology, offering strategic recommendations on how the U.S can coordinate and institutionalize trustworthy AI.

Against evolving threat actors in China and Russia, regulations and the cybersecurity industry remain out of sync, increasing the likelihood of continued harmful breaches of American government agencies and private companies. The industry needs a shake up, and "Overcoming the Challenges of Incentivizing Cybersecurity" suggests a new approach to cybersecurity regulation that will address industry needs and foster an economic climate in which innovation is not stifled. The "build up from the floor" approach aims to assist policymakers and regulators in starting a foundational set of regulations, then adding layers as impact is monitored. Its policy recommendations are designed to ensure both the public and private sectors can

effectively tackle evolving challenges from U.S competitors and adversaries.

While the Department of Defense has prioritized resilient supply chains for critical minerals, limited U.S. mining and refining capacity has led to dependence on imports from competitors like China. To address this challenge, "Materiel for Minerals: How the U.S. Can Leverage Security Assistance to Secure Supply Chains" introduces the materiel-for-minerals strategy, enabling the DoD to secure mineral production agreements in non-allied countries. This approach leverages tools like right-of-first-refusal offtake agreements in exchange for U.S. defense materiel that many countries desire.

Technologically sophisticated foreign actors such as Russia and China use influence campaigns as a disruptive tool to amplify discontent, shape election results, and blur the lines between fact and fiction. The rise of emerging technologies further exacerbates concerns over misinformation and disinformation, making detection even more challenging. "The Double-Edged Sword: How to Win the War on Fake News" examines the dual role of technology in both spreading and countering fake news and offers policy recommendations to strengthen the United States' ability to combat disinformation. While objectives in spreading fake news aren't always clear, countering efforts to manipulate American perceptions of domestic and foreign affairs remains essential.

While both the United States and China use emerging technologies to enhance their domestic security and expand foreign influence, China has been able to gain an advantage by exploiting U.S markets and innovations through espionage, cyber intrusions, and protectionist policies. Rather than countering, the U.S. and Europe have adopted broad tariffs and industrial policies, fueling global isolationism and protectionism, which stifles innovation globally. "Targeted and Precise: Innovation Versus Regulation in the Critical Technology Sector" ensure U.S. industrial controls are sufficiently targeted.

Discussions on emerging technologies often center on how competitors like China threaten to surpass the United States. However, flaws in determining who is ahead confuse interpretations of power and competition, which may pose indirect harm to understanding how the U.S can prioritize AI leadership in the long run. "How the U.S. Can Achieve Sustainable AI Leadership" explores aspects of AI development the United States should prioritize, such as aligning innovation with democratic values and making substantial investments in sustainable resources.

The artificial intelligence field is dominated by an obsession over machine learning, which is an important – but fundamentally limited – method to achieve AI leadership. The United States should expand its focus to the next innovative research area, neuro-symbolic AI. "American AI Leadership Should Not Be Defined by Machine Learning" aims to guarantee American AI research is not stuck with machine learning and the narrow pursuit of artificial general intelligence, but able to adapt to new frontiers that could solidify an enduring global leadership position in AI. This report integrates recommendations like utilizing existing programs such as The National Artificial Intelligence Initiative Office and creating new research institutes to realize this outcome.

These analyses reveal both the complexity of U.S.-China technological competition and the need for a coordinated, forward-looking response. While each report addresses distinct technological domains, several common themes emerge that should guide U.S. policy.

First, the United States must balance security imperatives with the openness that has driven American innovation for decades. Overly broad restrictions can stifle the very technological advancement they aim to protect. Instead, targeted and precise approaches to regulation, export controls, and investment screening are needed to address specific vulnerabilities without undermining the broader innovation ecosystem.

Second, securing America's technological future requires looking beyond current paradigms. Whether in artificial intelligence, cybersecurity, or countering disinformation, tomorrow's challenges will not be met with today's technological approaches alone. U.S. policy must support frontier research in emerging fields like neuro-symbolic AI while building resilience into critical technological infrastructure.

Third, the United States cannot win this competition alone. Partnerships with allies and like-minded nations are essential to developing shared technological standards, securing supply chains, and establishing norms within the technological world that align with democratic values. International collaboration will amplify America's technological strengths while distributing the burden of countering China's advancing capabilities.

Maintaining technological leadership is not just about producing more advanced technologies faster than competitors. It requires aligning technological development with values like transparency, privacy, and fairness that reflect America's principles. Technologies that embody these values will ultimately prove more resilient and widely adopted than alternatives developed under authoritarian systems.

The Tech Sovereignty & Security Portfolio at the New Lines Institute for Strategy and Policy will continue to bridge the gap between technical expertise and policy as we collectively confront these challenges. Our ongoing research will delve deeper into the issues presented in this compendium and explore additional domains critical to U.S. technological leadership, including biotechnology, quantum computing, and space security. By providing timely, targeted analysis grounded in deep technical understanding, we aim to support policymakers in making informed decisions that secure America's technological future and advance its values on the global stage. The technological race with China is not simply about who develops scientific capabilities first and who can produce the largest quantity but rather about shaping the technological landscape in ways that strengthen democracy, enhance security, and foster prosperity. With strategic foresight and coordinated action, the United States can maintain its technological leadership while ensuring that emerging technologies serve humanity's best interests.

About the Editors

Kelsey Quinn is the Program Head of Tech Sovereignty & Security at the New Lines Institute. She spearheads critical research into pragmatic mitigation of technological threats while preserving innovation needed for scientific advancement and competitiveness.

Prior to New Lines, Quinn contributed to the National Consortium for the Study of Terrorism and Responses to Terrorism (START). There she analyzed decision frameworks and attack scenarios of CBRN weapons on the DARPA Sigma+ project. At Michigan State University, her interdisciplinary research investigated bacterial pathogenesis and physiology in Vibrio cholerae, a Category B bioterrorism agent, combining her background in microbiology and security applications.

Quinn holds a Bachelor of Science in Microbiology with a minor in Global Terrorism from the University of Maryland and earned a master's in Security and Terrorism Studies from the same institution in 2024.

Eric Omorogieva is the Technology Policy Intern at the New Lines Institute, where he works on the Tech Sovereignty & Security portfolio. He is a graduate student at Johns Hopkins University's School of Advanced International Studies, pursuing a master's degree in international relations with concentrations in China studies and security, strategy, and statecraft. He holds a graduate certificate in Chinese and American studies at the Hopkins-Nanjing Center in Nanjing, China. He holds a 2021 bachelor's degree in politics and international affairs with minors in Chinese and African studies from Wake Forest University. Omorogieva is also a previous staff member of the International Rescue Committee, where he served refugee families in Washington, D.C.

Large rocks containing chromite are crushed before extracting and refining the ore that yields chromium at the Mughulkhil mine in Logar Province, Afghanistan, in September 2022. Chromium is a vital component of stainless steel. (Marcus Yam / Los Angeles Times)

Materiel for Minerals: How the U.S. Can Leverage Security Assistance to Secure Supply Chains

Jahara Matisek, Morgan Bazilian, Gregory Wischer

Introduction

The U.S. Department of Defense's (DoD) inaugural 2023 National Defense Industrial Strategy (NDIS) prioritizes "resilient supply chains," which include those for critical minerals.[1] These minerals are vital for the manufacture of DoD platforms like Virginia-class attack submarines and munitions like 155mm artillery rounds.[2] In 2008, defense production manufacturers used an estimated 275,000 tons of aluminum, over 200,000 tons of copper, and nearly 90,000 tons of lead.[3] Mineral consumption directed by the DoD will likely increase further as efforts to build more naval vessels,[4] munitions,[5] and uncrewed aerial vehicles continue.[6]

However, the limited U.S. mining and refining production capacity has led to heavy reliance on imports to meet demand.[7] The United States imports, largely from China, more than 95% of its demand for rare earth elements, which are used in DDG-51

Aegis destroyers, F-35 Lightning aircraft, and other technologies.[8] This dependence on mineral imports leaves the U.S. defense industrial base vulnerable to supply chain disruptions, such as those created by export controls, civil unrest, and natural disasters. Yet, of the over 22,000 words in the NDIS, "minerals" and "rare earth elements" are mentioned only four times.[9]

In 2024, the DoD released its NDIS Implementation Plan, which recommends stockpiling and investment in mineral projects to build more resilient U.S. mineral supply chains.[10] However, the National Defense Stockpile can only be tapped during national emergencies,[11] and the DoD can only award Defense Production Act (DPA) grants for mineral projects to the four countries deemed a "domestic source" – the United States, Canada, Australia, and the United Kingdom.[12] The DoD can indeed rely largely on domestic and allied mineral supplies, but for a small group of minerals, including bismuth and tin, production in both the United States and its allies is limited, forcing it to rely heavily on non-allied countries.

China is the world's largest producer of bismuth, which is used in defense alloys and machine tooling,[13] and the largest source of U.S. bismuth imports.[14] Similarly, China is the globe's largest producer of tin, used as an alloy in bearings.[15] Peru, Bolivia, and Indonesia are the largest sources of U.S. tin imports.[16] Thus, the DoD needs to source certain minerals from non-allied countries; however, it lacks the mechanisms to do so.

The DoD could seek new authorities and additional appropriations from Congress to award DPA grants to prospective mineral projects in non-allied countries, just as it currently does in Canada.[17] But in non-allied countries, both prospective mineral projects and producing mines face stoppage risks, like civil unrest and government disputes, as seen in Mozambique with graphite mines, New Caledonia with nickel mines, and Panama with a major copper mine.[18] In allied countries, too, like Canada and Australia, prospective mineral projects confront risks in commissioning and ramping up production. Therefore, DoD investment in mineral projects does not guarantee mineral production or sustained access to mineral production. Furthermore, even if Congress deems other countries as domestic sources and hence eligible for DPA grants, the administration of President Donald Trump could prioritize allocating funds to domestic mineral projects.[19]

The DoD could, however, seek offtake agreements for uncontracted mineral production in non-allied countries. Specifically, it could seek right-of-first-refusal (ROFR) offtake agreements, which would give it the right but not the requirement to buy a certain volume of minerals at market prices. The DoD could exercise its right to offtake following supply cutoffs – such as when China imposes mineral export bans[20] – and then sell the minerals at the same prices to U.S. defense firms. The DoD could also procure minerals and distribute them to defense firms responsible for high-priority defense programs facing mineral shortages and, hence, delays.

To secure these ROFR offtake agreements, the DoD could leverage its security assistance by conditioning U.S. security assistance, military cooperation (e.g., exercises and training), and foreign military sales (FMS) to mineral-rich countries on ROFR offtake agreements. Many foreign governments highly desire U.S. military training, cooperation, and arms. From fiscal year 2018 to fiscal year 2022,[21] FMS – which includes U.S.-funded sales – totaled nearly $250 billion.[22] The United States also spent over $68 billion on security assistance from 2018 to 2022,[23] and it provided security training to over 365,000 personnel from 2015 to 2019.[24] These engagements can deepen U.S. global security ties and, when leveraged effectively, secure U.S. mineral supply chains.

Importantly, many governments in countries that possess minerals lacking in the United States and allied countries seek U.S. defense materiel (officially, "defense articles"), and many of these same governments are shareholders in mineral projects in their countries. Thus, the DoD could offer materiel-for-minerals (M4M) deals. In exchange for FMS deals and other forms of security assistance (e.g., military training, education), the DoD can require ROFR offtake agreements for specific volumes of existing mineral production. M4M deals would provide the DoD, and thus the defense industrial base, access to additional mineral supplies in the event of significant demand or limited supply. Given the Trump administration's February 2025 decision to pursue a minerals deal with the Ukrainian government in exchange for continued

U.S. security assistance to Ukraine, this represents the first modern M4M case by the U.S. government.[25]

M4M deals could offer an innovative approach to securing mineral supply chains for the DoD. By leveraging existing security assistance programs and military equipment transfers, the M4M strategy aims to establish mutually beneficial agreements with mineral-rich countries, reducing U.S. dependence on minerals from adversarial countries. While M4M deals may appear overly transactional and at odds with typical norms, such arrangements are no different than past U.S. administrations that worked out de facto deals with Persian Gulf countries to ensure the flow of oil and natural gas out of the region in exchange for American military assistance and a security umbrella.

America's Vulnerable Mineral Supply Chains

Limited domestic mineral supplies constrain the U.S. defense industrial base. The United States no longer mines and refines many minerals despite having significant reserves and a long history of refining. For example, the United States stopped mining tantalum in 1959,[26] niobium in 1960,[27] and tungsten in 2015,[28] and it stopped refining primary gallium in 1987,[29] tin in 1989,[30] and primary bismuth in 1997.[31] Moreover, new mineral projects in the United States face long lead times. S&P Global estimates that the time from first discovery to first production for a mining project in the United States is 29 years.[32] Thus, the United States faces constraints in supplying the defense industrial base's mineral demands.

The United States relies heavily on mineral imports. For 31 of the 50 minerals on the U.S. critical minerals list, imports are used to meet over 50% of U.S. consumption, and for another 12 critical minerals, imports supply 100% of U.S. consumption.[33] China – the United States' "most consequential strategic competitor" – is the largest source of U.S. mineral imports.[34] Notably, imports are vulnerable to export controls, disruption, and delays, both in the country of production and on their shipping routes to the United States.[35]

In the country of production, export-focused mineral projects can face issues including royalty disputes with the host government and protests by the local community.[36] As another example, China has imposed export controls on certain minerals to the United States amid intensifying geopolitical tensions.[37] In December 2024, China outright banned exports of antimony, gallium, and germanium to the United States,[38] which relies heavily on China for these minerals.[39] Other governments – like Indonesia, Tanzania, and Zimbabwe – have imposed export bans on certain mineral ores and concentrates, too, seeking to encourage more processing and refining in their countries.[40]

Mineral imports are also vulnerable to shipping disruptions and delays. For instance, civil unrest in Mozambique has disrupted transport routes for Syrah's graphite mine in Balama, leading Syrah to default on its loans with the U.S. International Development Finance Corporation and the U.S. Department of Energy.[41]

Inadequate DoD Plans and Policies

To build more resilient mineral supply chains, the NDIS Implementation Plan recommends stockpiling and investing in mineral projects.[42] A more robust National Defense Stockpile could indeed support the defense industrial base, but this stockpile can only be tapped during national emergencies like war.[43] It is not meant to "insulate private industry from supply shocks."[44] For example, if priority defense programs face limited commercial supplies of minerals, the National Defense Stockpile could not release minerals to the defense firms executing the program unless a war or national emergency is declared.

The DoD could invest in mineral projects through programs like the DPA and the Industrial Base and Sustainment program.[45] However, the DoD can award grants to mineral projects only in the four countries considered to be domestic sources.[46] Although the DoD can generally depend on the United States and allied countries for most minerals given their collective reserves, recycling, and substitutes, the United States and its allies heavily rely on other countries for a select group of minerals.

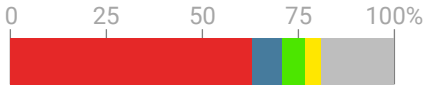
Yet, the DoD currently lacks policies to secure mineral supplies from these non-allied partner countries. It could seek new authority and additional appropriations

U.S. Mineral Reserves

Antimony

Years of domestic supply: 2.7 **U.S. import reliance:** 80%

Import Sources (2019-2022)
China Belgium India
Bolivia Other

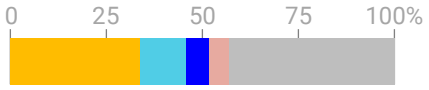


Largest Producers (mine production):
China, Tajikistan, Türkiye, Myanmar, Russia

Chromium

Years of domestic supply: 1.7 **U.S. import reliance:** 74%

Import Sources (2019-2022)
South Africa Kazakhstan
Canada Russia Other

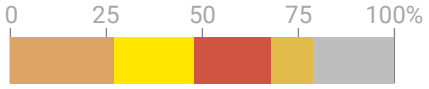


Largest Producers (mine production):
South Africa, Kazakhstan, Türkiye, India, Finland

Tin

Years of domestic supply: 0 **U.S. import reliance:** 74%

Import Sources (2019-2022)
Peru Bolivia Indonesia
Malaysia Other



Largest Producers (mine production):
China, Myanmar, Indonesia, Peru, Bolivia, Brazil

Bismuth

Years of domestic supply: 0 **U.S. import reliance:** 94%

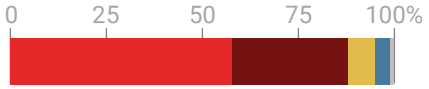
Import Sources (2019-2022)
China South Korea
Belgium Mexico Other

Largest Producers (refinery production):
China, Laos, South Korea, Japan, Kazakhstan

Arsenic

Years of domestic supply: 0 **U.S. import reliance:** 100%

Import Sources (2019-2022)
China Morocco Malaysia
Belgium Other

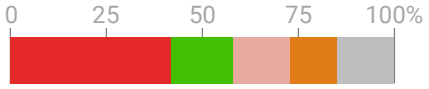


Largest Producers (arsenic trioxide production):
Peru, China, Morocco, Belgium, Russia

Graphite (natural)

Years of domestic supply: 0 **U.S. import reliance:** 100%

Import Sources (2019-2022)
China Mexico Canada
Madagascar Other

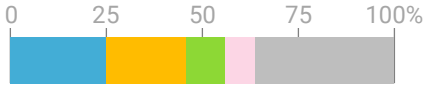


Largest Producers (mine production):
China, Madagascar, Mozambique, Brazil, South Korea

Manganese

Years of domestic supply: 0 **U.S. import reliance:** 100%

Import Sources (2019-2022)
Gabon South Africa
Australia Georgia Other



Largest Producers (mine production):
South Africa, Gabon, Australia, Ghana, China

Yttrium

Years of domestic supply: 0 **U.S. import reliance:** 100%

Import Sources (2019-2022)
China Germany France
South Korea Other

Largest Producers (mine production):
China, Myanmar

Years of domestic supply is calculated with amount of reserves to annual consumption

Note: The criteria for inclusion on this list are (1) the United States is over 50% import-reliant, (2) the United States has less than 5 years of domestic reserves to meet annual consumption, and (3) non-allies represent more than 50% of U.S. import sources. To calculate America's reserve supply, the U.S. Geological Survey must have data on reserves and annual consumption. Thus, the list excludes minerals—including cesium, rubidium, scandium, and tungsten—for which the U.S. Geological Survey lacks U.S. reserve and/or consumption data, but the United States potentially has reserves of these minerals.

Source: Kateryna Klochko

from Congress to give DPA awards to projects in these countries. For instance, the National Defense Authorization Act for fiscal year 2024 added Australia and the United Kingdom as domestic sources,[47] and the Additional Ukraine Supplemental Appropriations Act of 2022 appropriated $600 million to the DPA, including for strategic and critical materials.[48] However, it's not a given that Congress would add more countries to that list – even allies like New Zealand – and appropriating more DPA money is not assured.

Finally, investment in prospective commercial projects does not ensure production or continued access to production. Projects face production risks, including technical (e.g., ramping up, personnel), financial (e.g., low mineral prices impacting project feasibility), and governmental (e.g., permits, licenses) issues. For example, Australian company Jervois halted the opening of its Idaho Cobalt Operation due to low cobalt prices,[49] which the U.S. government attributed to overproduction by China.[50] Moreover, even if Congress deems other countries as domestic sources eligible for DPA grants, the Trump administration could still prioritize allocating funds to domestic mineral projects, given the president's support for onshoring.[51]

The Rationale for M4M Deals

The DoD could pursue offtake agreements for uncontracted mineral production in non-allied countries. Although some mines in these countries may already have other offtake agreements, it's likely there is uncontracted production capacity the DoD could secure through new agreements. In particular, the DoD could aim to sign ROFR offtake agreements, which would give it the option but not the obligation to purchase a specific volume of minerals before they are offered to other buyers at the same price. ROFR offtake agreements are common with prospective mineral projects, but such projects often face significant risks in achieving actual mineral production. Consequently, the DoD should focus on securing offtake agreements from existing mines to ensure a reliable mineral supply.

With ROFR offtake agreements, the DoD could exercise its right to offtake – for example, following supply cutoffs imposed by China[52] – and then sell the minerals to the defense industrial base. Outside of supply cutoffs, the DoD could exercise its right to offtake minerals and sell the minerals to defense firms executing priority defense programs but lacking access to adequate mineral volumes and facing corresponding delays. Alternatively, when the defense industrial base can access sufficient mineral volumes, the DoD does not have to execute ROFR offtake agreements. Simply put, ROFR offtake agreements effectively act as a buffer mineral supply that the DoD can tap when necessary.

To secure ROFR offtake agreements, the DoD could invest in mineral projects. Many foreign governments want increased investment in their mineral sectors; thus, direct investment may encourage mines with state ownership to sign ROFR offtake agreements. However, the DoD is restricted from issuing grants mineral projects outside of the United States, Canada, Australia, and the United Kingdom. Furthermore, even if investment in other countries was made possible, it would be considered risky given the operational and jurisdictional risks with mineral projects. Consequently, the DoD should avoid directly investing in overseas mineral projects in non-allied countries.

Instead, the DoD could be leveraged to offer arms sales and security training to non-allied countries in exchange for mineral agreements. For example, the DoD in tandem with the Department of State (DoS) can condition certain FMS on securing ROFR offtake agreements. Many governments in non-allied countries want to acquire U.S. defense articles, giving the DoD and DoS leverage to negotiate such agreements, assuming Congress will also consent to such deals. Importantly, many of these governments hold significant shares in mineral projects in their countries; therefore, they can negotiate such offtake agreements.

For instance, the Kazakh government, which has requested to buy U.S. defense articles,[53] has the largest stake in the Eurasian Resources Group (ERG),[54] which is a major producer of chromite in Kazakhstan.[55] Similarly, the Indonesian government is a major U.S. arms purchaser,[56] and Indonesia's state-owned holding mining company, Mining Industry Indonesia (MIND ID), has ownership stakes in several major mineral projects, including for tin.[57] These foreign governments exercise significant influence over their mineral projects. Given the lack of chromite and tin production

in the United States and allied countries, these minerals are targets for ROFR offtake agreements.

Importantly, the foreign government counterparty could hold ownership stakes in mineral projects in not only the home country but also in third-party countries. For example, the Kazakhstan government, through ERG, has ownership stakes not only in Kazakh projects but also in those in Africa and Brazil.[58] A hypothetical ROFR offtake agreement could feature a project with ownership stakes held by a foreign government outside that government's own country, too.

The DoD should negotiate M4M deals with foreign governments as means of providing itself, and thus the defense industrial base, with access to additional mineral supplies as needed. Using the FMS process to secure ROFR offtake agreements also leverages existing role of the DoS – primarily through the respective U.S. embassy's Office of Defense Cooperation – in the FMS process and Minerals Security Partnership.[59] M4M deals would strengthen both U.S. military partnerships and mineral supply chains. These deals could also help limit China's access to overseas mineral supplies by locking up mineral supplies that Chinese companies could previously have tapped.

Considering that the first Trump administration was particularly active in facilitating FMS deals and strengthening U.S. mineral supply chains, the current Trump administration will likely remain open to such deals.[60] Furthermore, the administration may support M4M deals because they are cost-neutral to the U.S. government, as seen with the tentative minerals deal with Ukraine in February 2025.

Using Foreign Military Sales to Secure Minerals

The FMS program involves selling and exporting American-made defense articles to eligible foreign purchasers, and a similar process of direct commercial sales could also be leveraged within the construct of M4M.[61] Defense articles include not only platforms, munitions, and their components but also properties, materials, and equipment that support military assistance, as well as machinery and tools for manufacturing defense articles.[62] The FMS program is governed by the Foreign Assistance Act of 1961,[63] International Security Assistance and Arms Export Control Act of 1976,[64] subsequent amendments, federal regulations like the U.S. Munitions List, and executive branch policies, including the Conventional Arms Transfer (CAT) policy.[65] The Security Assistance Management Manual (SAMM) then provides DoD with guidance on managing and implementing the FMS program.[66]

In the FMS program, the DoD acts as an intermediary by procuring defense articles on behalf of foreign purchasers. While these counterparts ultimately pay for the defense articles, they benefit from the DoD's technical and acquisition expertise. The Defense Security Cooperation Agency (DSCA) within the DoD manages the FMS program, ensuring proper accounting procedures and that all transactions align with U.S. defense and foreign policy objectives.

The FMS program is overseen by the DoS, which has the responsibility to notify Congress about certain deals. This process provides transparency and allows Congress to review the terms of significant FMS transactions.[67] Although Congress has the authority to review, block, and restrict these deals, these legislative actions are subject to presidential veto, highlighting the executive branch's ultimate control over arms transfers. Other arms transfer programs, including Foreign Military Financing and Excess Defense Articles, are also classified under the FMS program.[68]

Demand has increased for FMS since Russia invaded Ukraine in 2022.[69] In the government's fiscal year 2023, the FMS program totaled $66.2 billion in sales, with over $80 billion in 2024.[70] In the first two weeks of October 2024, for example, the DSCA approved selling MK 54 MOD 0 lightweight torpedoes to India;[71] the Electronic Attack Mission System to Italy;[72] Sentinel radar systems to Romania;[73] AIM-9X Block II Sidewinder missiles, AGM-114R3 Hellfire II missiles, ammunition for artillery systems, machine guns, and tanks to Saudi Arabia;[74] and munitions for the Guided Multiple Launch Rocket System and Army Tactical Missile System to the United Arab Emirates.[75]

The FMS process begins with a letter of request sent by the eligible foreign purchaser to a U.S. security cooperation organization, usually the Office of Defense

A general view of granite being mined on Feb. 26, 2025, in the Zhytomyr region of Ukraine. (Kostiantyn Libero v / Libkos / Getty Images)

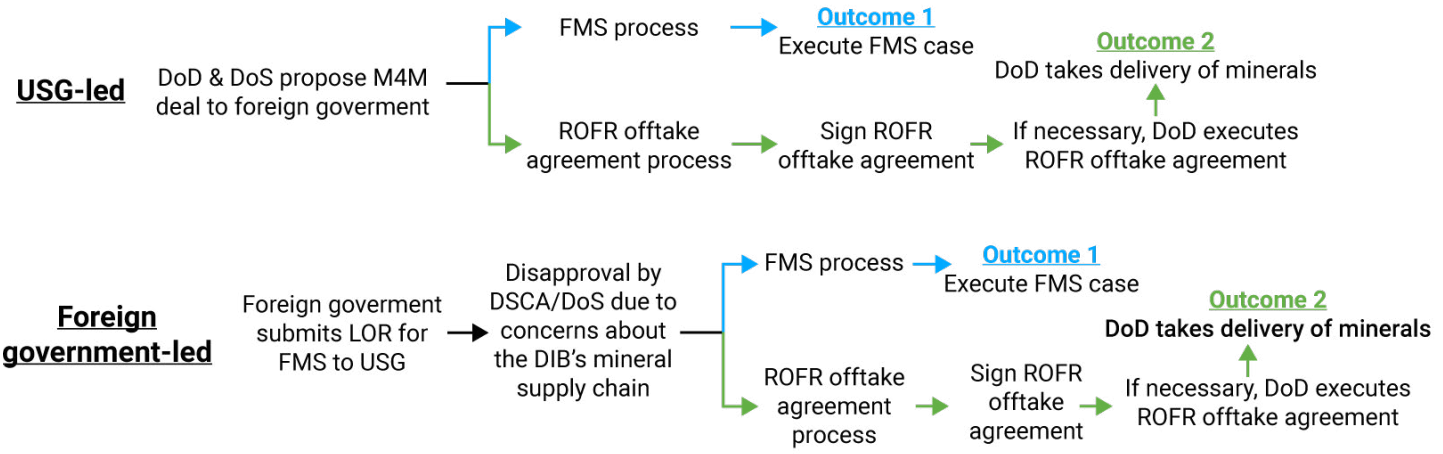
Cooperation, or directly to the DCSA or other relevant U.S. government agency.[76] The letter includes the foreign purchaser's desired defense articles. While the FMS process begins there, the U.S. government can indeed signal its support for FMS deals, effectively encouraging foreign purchasers to pursue them.[77] For instance, Trump, in his first administration, was vocal in his support of selling defense articles to foreign governments, such as Saudi Arabia.[78]

Upon receipt of the letter of request, the requisite U.S. government agency, usually the DCSA, evaluates the proposed deal for compliance with stated U.S. national security goals, the ability of the purchasing nation to pay for the acquisition, and other criteria, including the purchasing nation's military interoperability with the U.S. military. The FMS case is then sent to the State Department, which evaluates the deal based on overall policy objectives and handles the requisite notification to Congress. Generally, DCSA handles the execution of FMS, while the State Department focuses on interagency cooperation and overall alignment with U.S. foreign policy goals.

For most FMS cases, the State Department must notify Congress before approving an FMS deal. As previously stated, Congress can block or restrict an FMS deal through a joint resolution. However, the president can veto the resolution. Additionally, the president (or the secretary of state with delegated authority) can issue a declaration of emergency and bypass congressional input. This action occurred in late 2023 when then-Secretary of State Antony Blinken utilized emergency authorities on a sale of 155mm artillery rounds to Israel "given the urgency of Israel's defensive needs."[79]

When the FMS case clears all approval processes, the U.S. government will acquire the defense articles on behalf of the foreign purchaser, which covers the full cost associated with the deal.[80] The DoD will sometimes pair FMS with other military assistance and training to further enhance the defense relationship and improve interoperability.

The Process of M4M Deals



Sources: Jahara Matisek, Gregory Wischer, Morgan Bazilian

M4M Deal Structure

The DoD could pursue M4M deals by linking ROFR mineral offtake agreements with FMS deals and other security assistance arrangements. The FMS process would remain unchanged, and the ROFR offtake agreement negotiation would run concurrently. Due to the DoD's discretion to approve FMS deals on a case-by-case basis, the DoD could condition specific FMS transactions on securing ROFR mineral offtake agreements.

Just as the DoD is an intermediary for the foreign eligible purchaser in FMS deals, it would also act as such in executing offtake agreements. A defense firm would request that the DoD execute a mineral offtake, and it would then determine whether it should and for what volume. The DoD could then use DPA funds to execute the purchase of minerals from non-domestic sources.[81] Under a DPA exemption, the DoD can purchase industrial resources – including minerals – "necessary to assure the availability to the United States of overseas supplies."[82] This exemption exempts the DoD from other laws, such as restricting contract solicitations to domestic sources.[83]

Defense firms would be responsible for paying the resulting costs, including duties; therefore, both FMS deals and ROFR offtake agreements would be cost-neutral, meaning no additional expenditures are incurred by the U.S. government. After taking delivery of the minerals, the DoD would resell them to the requesting defense firm. The DoD would have to develop corresponding procedures for considering offtake requests, including how to adjudicate multiple bids for limited mineral volumes.[84]

Notably, then-President Joe Biden signed a waiver of DPA purchase requirements for critical and strategic materials, suspending purchase requirements such as a presidential determination, spending limitations, and congressional notifications.[85] The current administration could now sign and, if necessary, execute ROFR mineral offtake agreements.

To discourage foreign counterparts from reneging on mineral offtake agreements after receiving defense articles, the DoD could withhold spare parts. Under the current CAT policy, the DoD can at any time "cease the transfer of or future support for a transferred defense article or service."[86] The DoD could condition security assistance and training programs, too, on the foreign government upholding ROFR offtake agreements. Additionally, if foreign governments seek to circumvent ROFR offtake agreements by procuring defense articles directly from U.S. arms manufacturers via Direct Commercial Sales licenses, the State Department can determine that those sales must "be required to proceed through the FMS process."[87]

The proposed M4M deal structure complies in principle with existing statutes. The Foreign Assistance Act says

that U.S. policy for security assistance is "based upon the principle of effective self-help and mutual aid,"[88] while the AECA states that FMS should "be approved only when they are consistent with the foreign policy of the United States,"[89] which includes strengthening U.S. supply chains for minerals.[90] The AECA adds that the deals should consider "the impact of the sales on programs of social and economic development,"[91] and mineral offtake agreements would indeed be economically beneficial to the foreign counterpart.

The M4M deal structure also aligns with the CAT policies of both Biden and the first Trump administration. Biden's CAT Policy supported U.S. efforts to "strengthen the United States manufacturing and defense industrial base and ensure resiliency in global supply chains."[92] The first Trump administration's CAT Policy was also explicit: arms transfers should "strengthen the manufacturing and defense industrial base."[93] Given the first Trump administration's CAT Policy, the current Trump administration could issue a CAT policy that emphasizes the importance of arms transfers in strengthening the defense industrial base – which M4M deals would do.

The security assistance portion of the M4M deal structure aligns with U.S. policy, too. Providing arms, training, and military equipment to a foreign government makes them more militarily effective, a core rationale for U.S. security assistance.[94] Such security assistance also increases U.S. military influence in increasingly important non-allied countries like Indonesia vis-à-vis China.[95]

Example M4M Deal: Indonesia

The DoD consumes an estimated 2,600 metric tons of tin annually.[96] Yet, the United States has not mined tin since 1993, and it has not smelted it since 1989.[97] The National Defense Stockpile contains 3,578 metric tons of tin as of September 30, 2022.[98] Consequently, the United States writ large relies on imports to meet 74% of its domestic demand for refined tin, with the other 26% of consumption being met by recycled tin.[99] Non-allied countries like Peru, Bolivia, and Indonesia are the largest sources of U.S. imports.[100]

Indonesia specifically is a major producer of tin,[101] and PT Timah Tbk, the country's largest tin producer, is majority-owned by the government of Indonesia.[102] Indonesia is also a major buyer of U.S. defense articles through the FMS program. In February 2022, the DSCA certified a nearly $14 billion deal for 36 F-15ID aircraft and related equipment.[103] DSCA has previously approved other Indonesian FMS deals involving MV-22 Osprey aircraft,[104] AIM-120C-7 missiles,[105] and AIM-9X-2 Sidewinder missiles.[106] The DoD could condition and entice future FMS deals with Indonesia based on the DoD signing a ROFR tin offtake agreement with PT Timah Tbk.

Other governments that the U.S. government could target with M4M deals are Arabian Gulf countries like Saudi Arabia and the United Arab Emirates. Traditionally, these countries are major purchases of U.S. defense articles, and while these countries are not major mineral producers, their state-owned enterprises – including state investment firms like Saudi Arabia's Manara Minerals – are taking significant stakes in mineral projects and companies in other countries. Therefore, the DoD could condition future FMS deals with these governments on them signing ROFR mineral offtake agreements. The DoD and State Department could identify other potential target governments that both produce minerals and want to purchase U.S. defense articles.

M4M Implementation

U.S. policymakers should consider the M4M approach as part of a broader strategy to secure America's mineral supply chains. This includes investing in domestic mineral production and processing capabilities, supporting research into alternative materials and recycling technologies, strengthening partnerships with allied nations to diversify supply chains, and developing comprehensive risk assessment and mitigation strategies for mineral supply disruptions. M4M deals simply offer another tool for addressing U.S. mineral supply chain vulnerabilities. However, its implementation must be carefully integrated into a comprehensive approach to mineral security and balanced against potential negative consequences.

Implementing the M4M strategy will require coordination among various U.S. government agencies, namely the DoD and DoS. Successful execution will

U.S. Secretary of State Antony Blinken and Norwegian Foreign Minister Espen Barth Eide sign a memorandum of cooperation on "High-Standard, Market-Oriented Trade of Critical Minerals," strengthening their partnership on clean energy, on Sept. 30, 2024, in Washington, D.C. (Kevin Dietsch / Getty Images)

depend on identifying suitable partner countries with both access to mineral resources and interest in obtaining U.S. military equipment and/or assistance. Negotiating agreements that balance mineral access with appropriate levels of military support will be crucial, as will ensuring compliance with existing laws and regulations governing arms sales and technology transfers. Developing mechanisms to monitor and enforce M4M agreements over time will also be essential for long-term success.

If the U.S. government indeed pursues M4M deals, it must be responsive to changing global conditions. Regular reassessment of the M4M approach, its impacts, and its alignment with broader U.S. foreign policy and national security objectives will be important. These reassessments could involve adjusting the terms of agreements, exploring new partnerships, or developing alternative strategies as geopolitical and economic landscapes evolve. The U.S. government should establish clear metrics for evaluating the effectiveness of M4M agreements and be prepared to modify or terminate arrangements that do not meet established goals or that generate negative consequences.

Lastly, the success of an M4M strategy will depend on robust oversight and accountability mechanisms. Transparent reporting on the outcomes of these agreements, including their impact on mineral supply chains, partner nation development, and regional stability will be essential for maintaining domestic and international support for the program.

Benefits and Risks

The M4M approach presents several benefits. It provides a mechanism for securing mineral access without requiring new legislative authorities or appropriations. It capitalizes on existing relationships and programs such as the FMS program to create mutually beneficial arrangements with mineral-rich countries. Furthermore, it offers flexibility through ROFR offtake agreements, allowing the DoD to access minerals without committing to unnecessary

purchases. Critically, M4M deals could reduce reliance on adversarial countries, namely China, for critical minerals.

The M4M strategy has the potential to reshape global mineral supply chains and influence geopolitical relationships to the United States' benefit. The DoD would not only strengthen its position in mineral-rich countries but also offer a demand alternative to China, helping diversify global mineral supply networks. U.S. allies could also adopt the M4M strategy and further lock out adversaries like China and Russia from accessing some mineral supplies.

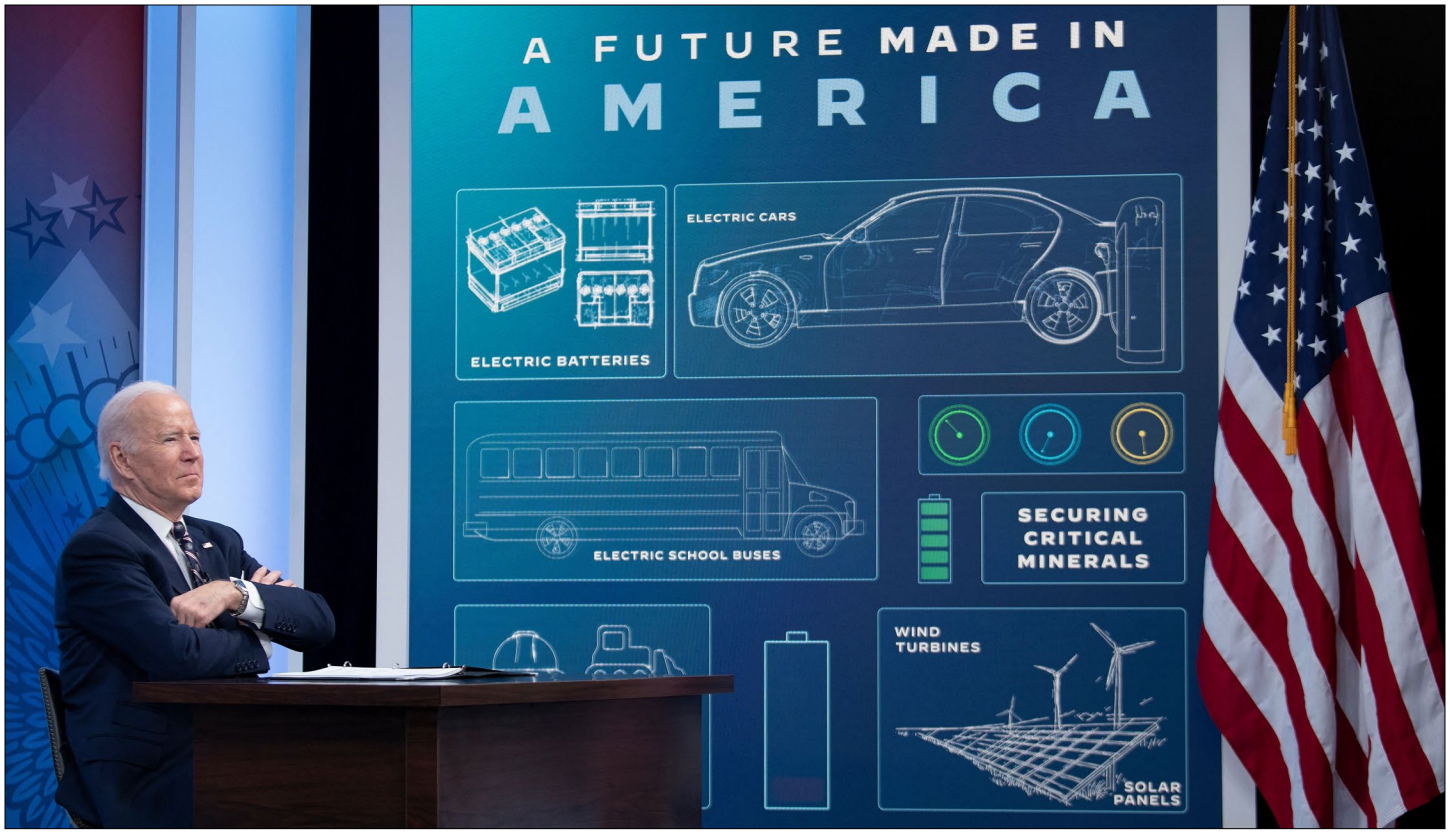
However, the M4M approach also poses risks. First, M4M deals for minerals lacking in the United States could dissuade investment in domestic stockpiling, recycling, and substitutes for those minerals. Domestic sources of minerals would be less prone to disruption than those from M4M deals, and they could also be transported to domestic defense firms more quickly, which is why domestic mineral production and stockpiling should be prioritized. The U.S. government, therefore, should view M4M deals as part of a broader strategy that includes developing domestic capabilities and fostering innovation in mineral extraction and processing technologies.

Second, exchanging military equipment for mineral access could exacerbate regional tensions and contribute to arms proliferation. Governments receiving advanced weaponry might use it to repress domestic populations or engage in armed conflict with neighboring countries; however, these very same governments may be dissuaded from acting in such a manner in order to maintain access to U.S. defense materiel. These actions could lead to increased violence and humanitarian crises, which contradict broader U.S. foreign policy goals of promoting peace and stability. Given the exchange of arms for minerals, other governments and international institutions may also view M4M deals as unethical and exploitative, harming U.S. diplomatic standing. Thus, the U.S. government must engage in careful diplomacy and transparent communication about the mutual benefits of M4M agreements.

Third, increased mineral extraction activities could harm the environment by contributing to deforestation, water pollution, and habitat destruction, among other effects. Moreover, local communities might face displacement as governments prioritize mineral production to secure military deals. These impacts could damage the United States' reputation and contravene its commitments to environmental protection and human rights. To mitigate these risks, ROFR mineral offtake agreements could include provisions that require environmental protection and community engagement.

Policy Recommendations

1. **The White House should update its CAT policy to emphasize that one of the objectives of its arms transfers policy is to strengthen the defense industrial base's supply chains, including for critical minerals.** The Trump administration could be amenable to such an update since during the president's first term, CAT policy noted that the arms transfer action plan "should account for the competitive environment in which the United States must operate and the need to protect and expand our technological advantages and our defense industrial base."[107] The mineral supply chains of the defense industrial base are vulnerable; therefore, the U.S. government's arms transfer policy could help protect these supply chains and, hence, the defense industrial base.
2. **State Department leadership should direct its chiefs of mission and their requisite country teams to prepare Integrated Country Strategies (ICSs) that explicitly include M4M deals.**[108] An ICS is the four-year strategy that articulates priorities in a given country, including mission goals and objectives for arms transfers and other cooperation.[109] Drafting the ICS is led by the chief of mission and includes input from other relevant government agencies, including the DoD. By including M4M deals in an ICS, U.S. embassies around the world would have direct tasking to pursue those deals. Embassy teams would also be responsible for favorably framing these deals as mutually beneficial with the foreign counterparts.
3. **DoD's Manufacturing Capability Expansion & Investment Prioritization Office should develop a list of target minerals and corresponding target countries for M4M deals.** This list of minerals



U.S. President Joe Biden speaks during a virtual meeting on securing critical mineral supply chains in Washington, D.C., on Feb. 22, 2022. (Brendan Smialowski / AFP via Getty Images)

lacking in both the United States and allied countries would be distributed to the U.S. embassy teams in target countries. Additionally, the office oversees the DPA Title III program, which would be used to execute the ROFR mineral offtake agreements. Consequently, the office would be responsible for drafting procedures for receiving and reviewing requests to execute these offtake agreements, as well as determining mineral allocations to requesting defense firms.

4. **State Department leadership should assign responsibilities for drafting preliminary M4M deals to the economic sections and Offices of Defense Cooperation at U.S. embassies.** The economic sections at U.S. embassies understand the mining industries in the host countries, while the security cooperation offices understand the host countries' interests in U.S. defense articles. The draft deals would then be sent to State Department and Defense Department headquarters for final drafting before being presented to the foreign counterparts. The embassy teams would then be responsible for negotiating the M4M deal, subject to final approval by DoD and State Department leadership.
5. **The DSCA should issue a policy memo on minerals, noting that letters of request for FMS deals can be denied due to concerns about the mineral supply chains of the U.S. defense industrial base.** This policy memo can be used as a predicate for the DSCA and State Department to deny FMS letters from foreign governments with whom the DoD seeks ROFR mineral offtake agreements. The disapproval notice would effectively notify the foreign government that the U.S. government would reconsider the request if the foreign government signed an ROFR offtake agreement.

Conclusion

The DoD faces significant challenges in securing its mineral supply chains, which are crucial in both defense platforms and munitions. The DoD's reliance on foreign mineral sources poses substantial risks to the defense industrial base and, by extension, U.S.

national security. The proposed M4M deal framework offers an option for mitigating these risks.

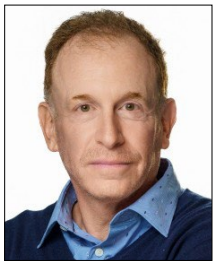
By carefully implementing and continuously refining the M4M deal structure over time, the DoD has the potential to strengthen its global partnerships and secure its mineral supplies in an increasingly competitive world. However, success will require sustained commitment, careful diplomacy, and a willingness to address the ethical and practical challenges that arise from linking military assistance to mineral extraction.

Future research on M4M deals could focus on assessing the legal and regulatory frameworks necessary to support M4M deals, to include expanding direct commercial sales within the same construct, analyzing the potential economic impacts on both the defense industrial base and partner nations, evaluating the environmental and social impacts of increased mineral extraction in partner countries, and exploring alternative strategies for securing mineral supplies, including increased domestic production and recycling initiatives

As U.S.-China competition intensifies and the defense industrial base's mineral demand grows, M4M deals could provide the DoD with another tool to strengthen the supply chains of the defense industrial base.

U.S. Air Force Lt. Col. Jahara "Franky" Matisek is a senior pilot who has a Ph.D. in Political Science from Northwestern University. He is currently a military professor at the U.S. Naval War College, fellow at The Payne Institute for Public Policy, and will be assigned next to the J3 at NORTHCOM. Matisek was previously an associate professor at the U.S. Air Force Academy and is the most published active-duty officer, with two books and over 100 articles in peer-reviewed journals and policy relevant outlets on warfare, strategy, and security assistance.

The views expressed are those of the authors and do not reflect the official position of the U.S. Air Force, U.S. Naval War College, Department of Defense, or the U.S. Government. This article was supported by the Air Force Office of Scientific Research under award number FA9550-20-1-0277.



Morgan D. Bazilian is director of the Payne Institute and professor of public policy at the Colorado School of Mines. Previously, he was lead energy specialist at the World Bank. He has over two decades of experience in energy security, natural resources, national security, energy poverty, and international affairs. He holds a Ph.D. in energy physics and was a Fulbright Fellow. He is a member of the Council on Foreign Relations, a global fellow at the Woodrow Wilson International Center, and an adjunct professor of thermal physics at University College Cork. He is a board member of the Veterans Advanced Energy Project, and he holds a joint appointment at NREL on the topic of energy security.

Gregory Wischer is the founder and principal of Dei Gratia Minerals, a critical minerals consulting firm. He is also a non-resident fellow at the Payne Institute for Public Policy at the Colorado School of Mines and a non-resident fellow at the Northern Australia Strategic Policy Centre at the Australian Strategic Policy Institute. Previously, Wischer was executive vice president at an American company building a nickel-cobalt metal refinery in the United States. He received his bachelor's in International Business from Boise State University, and he received his master's in security studies from Georgetown University.

Endnotes

1 U.S. Department of Defense, "National Defense Industrial Strategy," 2023, https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf.

2 Valerie Bailey Grasso, "Rare Earth Elements in National Defense: Background, Oversight Issues, and Options for Congress," R41744, Congressional Research Service, September 17, 2013, https://www.everycrsreport.com/files/20130917_R41744_f524dd012737e617d9a79c8bf3a62ad071a52904.pdf; and James McKeigue, "Russia's War in Ukraine Boosts Copper Demand," Fastmarkets, July 8, 2024, https://www.fastmarkets.com/insights/russias-war-in-ukraine-boosts-copper-demand/.

3 Institute for Defense Analyses, "Key Materials for High-Priority Weapon Systems, and Assessing Risks to Their Supply: A Report for the U.S. Defense National Stockpile Center," July 31, 2008, in U.S. Department of Defense, "Reconfiguration of the National Defense Stockpile Report to Congress," April 2009, B-2, https://www.scribd.com/document/16483302/Reconfiguration-of-the-National-Defense-Stockpile-Report-to-Congress.

4 Paul McLeary and Connor O'Brien, "Exclusive: Navy Projects Fleet Will Expand to nearly 400 Ships," POLITICOPro, March 19, 2024, https://subscriber.politicopro.com/article/2024/03/navy-projects-fleet-will-expand-to-nearly-400-ships-00147840.

5 Josh Luckenbaugh, "Just in: Army Modernizing, Expanding Munitions Production Facilities," National Defense Magazine, February 5, 2024, https://www.nationaldefensemagazine.org/articles/2024/2/5/army-modernizing-expanding-munitions-production-facilities.

6 Jen Judson, "Army Picks Two Companies to Get Small Drones to Brigade Combat Teams," DefenseNews, September 12, 2024, https://www.defensenews.com/land/2024/09/12/army-picks-two-companies-to-get-small-drones-to-brigade-combat-teams/.

7 Nedal T. Nassar, Elisa Alonso, and Jamie L. Brainard, "Investigation of U.S. Foreign Reliance on Critical Minerals—U.S. Geological Survey Technical Input Document in Response to Executive Order No. 13953 Signed September 30, 2020," Report 2020–1127, U.S. Geological Survey, revised December 7, 2020, 2, https://pubs.usgs.gov/of/2020/1127/ofr20201127.pdf.

8 Daniel J. Cordier, "Rare Earths," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 144, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-rare-earths.pdf; and Valerie Bailey Grasso, "Rare Earth Elements in National Defense: Background, Oversight Issues, and Options for Congress," R41744, Congressional Research Service, September 17, 2013, https://www.everycrsreport.com/files/20130917_R41744_f524dd012737e617d9a79c8bf3a62ad071a52904.pdf.

9 The Nationa Defense Industrial Strategy—with over 22,000 words—only mentions "minerals" and "rare earth elements" four times. See U.S. Department of Defense, "National Defense Industrial Strategy," 2023, 8, 17–18, 43, https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf.

10 U.S. Department of Defense, "National Defense Industrial Strategy: Implementation Plan for FY2025," 2024, 19, 25, 30–32, 69, 80, https://www.businessdefense.gov/docs/ndis/NDIS-Implementation-Plan-FY2025.pdf.

11 50 U.S.C. §98a(b), https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AU.S. C-prelim-title50-section98a&num=0&saved=%7CKHRpdGxlOjUwIHNlY3Rpb246OTggZWRpdGlvbjpwcmVsaW0p%7C%7C%7C0%7Cfalse%7Cprelim.

12 50 U.S.C. §4552(7), https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter55&edition=prelim.

13 Under Secretary of Defense for Acquisition, Technology and Logistics, "Strategic and Critical Materials 2015 Report on Stockpile Requirements," U.S. Department of Defense, January 2015, appendix 6-9, https://www.hsdl.org/?view&did=764766.

14 Amy C. Tolcin, "Bismuth," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 46–47, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-bismuth.pdf.

15 Under Secretary of Defense for Acquisition, Technology and Logistics, "Strategic and Critical Materials 2015 Report on Stockpile Requirements," U.S. Department of Defense, January 2015, appendix 6-85, https://www.hsdl.org/?view&did=764766.

16 Chad A. Friedline, "Tin," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 184–185, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-tin.pdf.

17 The U.S. Department of Defense has committed approximately $65 million in Defense Production Act grants to Canadian mineral projects. See "Department of Defense Awards $14.7 Million to Enhance North American Cobalt and Graphite Supply Chain," U.S. Department of Defense, May 16, 2024, https://www.defense.gov/News/Releases/Release/Article/3777044/department-of-defense-awards-147-million-to-enhance-north-american-cobalt-and-g/; "Department of Defense Awards $20 Million to Establish Sustainable Cobalt Sulfate Production for Large Capacity Battery Supply Chain," U.S. Department of Defense, August 19, 2024, https://www.defense.gov/News/Releases/Release/Article/3877791/department-of-defense-awards-20-million-to-establish-sustainable-cobalt-sulfate/; "Department of Defense Awards $12.9 Million to Increase Production of Active Materials for Lithium Iron Phosphate Cathodes," U.S. Department of Defense, September 26, 2024, https://www.defense.gov/News/Releases/Release/Article/3917579/department-of-defense-awards-129-million-to-increase-production-of-active-mater/; and "Department of Defense Makes Investment to Strengthen the Tungsten Supply Chain," U.S. Department of Defense, December 13, 2024, https://www.defense.gov/News/Releases/Release/Article/4000947/department-of-defense-makes-investment-to-strengthen-the-tungsten-supply-chain/.

18 Paul-Alain Hunt and Amy Bainbridge, "Syrah Declares Force Majeure for Its Graphite Mine in Mozambique," Bloomberg, December 11, 2024, https://www.bloomberg.com/news/articles/2024-12-11/syrah-declares-force-majeure-for-its-graphite-mine-in-mozambique; Gus Trompiz, "Explainer: What New Caledonia Riots Mean for the Nickel industry," Reuters, May 22, 2024, https://www.reuters.com/markets/commodities/what-new-caledonia-riots-mean-nickel-industry-2024-05-22/; and Valentine Hilaire and Divya Rajagopal, "Explainer: What Happens Next after Panama's Top Court Strikes Down First Quantum Contract?" Reuters, November 28, 2023, https://www.reuters.com/markets/commodities/what-happens-next-after-panamas-top-court-strikes-down-first-quantum-contract-2023-11-28/.

19 Caroline Peachey, "Explainer: What Trump 2.0 Means for the Mining Industry," Mining Technology, November 7, 2024, https://www.mining-technology.com/features/explainer-what-trump-2-0-means-for-the-mining-industry/.

20 Gregory Wischer, Morgan Bazilian, and Jahara Matisek, "China's Mineral Export Ban Strikes at the U.S. Defense Industrial Base," The Diplomat, December 6, 2024, https://thediplomat.com/2024/12/chinas-mineral-export-ban-strikes-at-the-us-defense-industrial-base/.

21 The U.S. government's fiscal year is October 1–September 30.

22 Christina L. Arabia, Nathan J. Lucas, and Michael J. Vassalotti, "Transfer of Defense Articles: U.S. Sale and Export of U.S.-Made Arms to Foreign Entities," R46337, Congressional Research Service, updated March 23, 2023, 3, https://crsreports.congress.gov/product/pdf/R/R46337/4.

23 Center for International Policy, "Security Sector Assistance Database," accessed December 31, 2024, https://internationalpolicy.org/programs/sam/security-sector-assistance-database/.

24 Center for International Policy, "Foreign Military Training Database," accessed December 31, 2024, https://internationalpolicy.org/programs/sam/foreign-military-training-database/.

25 Jane Lytvynenko, Ian Lovett, and Alan Cullison, "U.S. and Ukraine Prepare to Sign Minerals Deal—with Critical Details Unresolved," Wall Street Journal, February 26, 2025, https://www.wsj.com/world/zelensky-says-details-of-u-s-deal-for-resources-still-need-to-be-worked-out-aa763dab.

26 Chad A. Friedline, "Tantalum," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 178, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-tantalum.pdf.

27 Chad A. Friedline, "Niobium (Columbium)," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 126, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-niobium.pdf.

28 Kim B. Shedd, "Tungsten," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 190, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-tungsten.pdf.

29 Brian W. Jaskula, "Gallium," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 74, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-gallium.pdf.

30 Chad A. Friedline, "Tin," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 184, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-tin.pdf.

31 Amy C. Tolcin, "Bismuth," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 46, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-bismuth.pdf.

32 Mohsen Bonakdarpour, Frank Hoffman, and Keerti Rajan, "Mine Development Times: The U.S. in Perspective," S&P Global, June 2024, 8, https://cdn.ihsmarkit.com/www/pdf/0724/SPGlobal_NMA_DevelopmentTimesU.S. inPerspective_June_2024.pdf.

33 U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 6, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024.pdf.

34 U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 6–7, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024.pdf; and U.S. Department of Defense, "2022 National Defense Strategy," October 27, 2022, iii, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf.

35 Gregory Wischer, Morgan Bazilian, and Jahara Matisek, "China's Mineral Export Ban Strikes at the U.S. Defense Industrial Base," The Diplomat, December 6, 2024, https://thediplomat.com/2024/12/chinas-mineral-export-ban-strikes-at-the-us-defense-industrial-base/.

36 Oliver Griffin and Steve Orlofsky, "Miner South32 Files Request for Arbitration in Colombia Royalty Dispute," Reuters, March 31, 2020, https://www.reuters.com/article/world/miner-south32-files-request-for-arbitration-in-colombia-royalty-dispute-idU.S. KBN21I33U/; and Marco Aquino and Elaine Hardcastle, "Protesters Blockade Peru's Las Bambas Mine after Talks Fall through," Reuters, April 10, 2024, https://www.reuters.com/world/americas/protesters-blockade-perus-las-bambas-mine-after-talks-fall-through-2024-04-10/.

37 For a list of minerals subject to China's export controls, see Gregory Wischer, "On November 15, 2024, China Ministry of Commerce...." LinkedIn, November 21, 2024, https://www.linkedin.com/posts/gregory-wischer-009887142_prc-export-control-lists-of-dual-use-items-activity-7265359130301710339-nkAJ?utm_source=share&utm_medium=member_desktop.

38 China's Ministry of Commerce, "Announcement No. 46 of 2024 of the Ministry of Commerce on Strengthening Export Control of Relevant Dual-Use Items to the United States," December 3, 2024, https://www.mofcom.gov.cn/zwgk/zcfb/art/2024/art_3d5e990b43424e60828030f58a547b60.html.

39 Kateryna Klochko, "Antimony," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 34, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-antimony.pdf; Brian W. Jaskula, "Gallium," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 74, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-gallium.pdf; and Amy C. Tolcin, "Germanium," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 80, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-germanium.pdf.

40 International Energy Agency, "Prohibition of the Export of Nickel Ore," updated March 19, 2024, https://www.iea.org/policies/16084-prohibition-of-the-export-of-nickel-ore; David Whitehouse, "Exclusive: Tanzania to Ban Unrefined Lithium Exports from May 2024," The Africa Report, November 2, 2023, https://www.theafricareport.com/326733/exclusive-tanzania-to-ban-unrefined-lithium-exports-from-may-2024/; and "Zimbabwe's Lithium Ore Export Ban Highlights Africa's Lithium Potential," Benchmark Source, December 23, 2022, "https://source.benchmarkminerals.com/article/zimbabwes-lithium-ore-export-ban-highlights-africas-lithium-potential.

41 Syrah Resources, "Balama Force Majeure," ASX announcement/media release, December 12, 2024, https://company-announcements.afr.com/asx/syr/76380d8f-b80e-11ef-8ebe-de7546lb6fbc.pdf.

42 U.S. Department of Defense, "National Defense Industrial Strategy: Implementation Plan for FY2025," 2024, 19, 25, 30–32, 69, 80, https://www.businessdefense.gov/docs/ndis/NDIS-Implementation-Plan-FY2025.pdf.

43 50 U.S.C. §98a(b)–(c), https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AU.S. C-prelim-title50-section98a&num=0&saved=%7CKHRpdGxlOjUwIHNlY3Rpb246OTggZWRpdGlvbjpwcmVsaW0p%7C%7C%7C0%7Cfalse%7Cprelim.

44 Bureau of Industry and Security, U.S. Department of Commerce, "Request for Public Comments on the Potential Market Impact of the Proposed Fiscal Year 2026 Annual Materials Plan From the National Defense Stockpile Market Impact Committee," Federal Register 89, no. 168 (August 29, 2024): 70167, https://www.govinfo.gov/content/pkg/FR-2024-08-29/pdf/2024-19422.pdf.

45 Wes Shinego, "DOD Leverages Defense Production Act to Galvanize Critical Supply Chains," U.S. Department of Defense, December 4, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3985393/dod-leverages-defense-production-act-to-galvanize-critical-supply-chains/.

46 50 U.S.C. §4552(7), https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter55&edition=prelim. Even mineral production in allied countries is not totally secure. but Canada in December 2024 appeared to threaten export controls on minerals to the United States amid a U.S.–Canada tariff row. Then Deputy Canadian Prime Minister Chrystia Freeland said, "Some premiers proactively identified products that their provinces produce and export to the United States and which the U.S. relies on and should be considered as part of the Canadian response. This included some critical minerals and metals." See CTV News, "Premiers Pushed for 'Robust Canadian Response' to Trump Tariffs Threat in Meeting with PM: Freeland," YouTube, December 11, 2024, https://www.youtube.com/watch?v=gI7G2lxKxLc&feature=youtu.be.

47 An Act to Authorize Appropriations for Fiscal Year 2024 for Military Activities of the Department of Defense and for Military Construction, and for Defense Activities of the Department of Energy, to Prescribe Military Personnel Strengths for Such Fiscal Year, and for other Purposes, Public Law 118–31, U.S. Statutes at Large 137 (2023): 415, https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf.

48 An Act Making Emergency Supplemental Appropriations for Assistance for the Situation in Ukraine for the Fiscal Year Ending September 30, 2022, and for Other Purposes, Public Law 117–128, U.S. Statutes at Large 136 (2022): 12114, https://www.congress.gov/117/plaws/publ128/PLAW-117publ128.pdf.

49 Jervois Global Limited, "Jervois Global Suspends Final Construction at Idaho Cobalt Operations," Junior Mining Network, March 29, 2023, https://www.juniorminingnetwork.com/junior-miner-news/press-releases/2313-tsx-venture/jrv/138634-jervois-suspends-final-construction-at-idaho-cobalt-operations.html.

50 Michael J. Kavanagh, "U.S. Blames China's CMOC for Predatory Tactics Behind Cobalt Glut," Bloomberg, May 14, 2024, https://www.bloomberg.com/news/articles/2024-05-14/us-blames-china-s-cmoc-for-predatory-tactics-behind-cobalt-glut.

51 Caroline Peachey, "Explainer: What Trump 2.0 Means for the Mining Industry," Mining Technology, November 7, 2024, https://www.mining-technology.com/features/explainer-what-trump-2-0-means-for-the-mining-industry/.

52 Gregory Wischer, Morgan Bazilian, and Jahara Matisek, "China's Mineral Export Ban Strikes at the U.S. Defense Industrial Base," The Diplomat, December 6, 2024, https://thediplomat.com/2024/12/chinas-mineral-export-ban-strikes-at-the-us-defense-industrial-base/.

53 Defense Security Cooperation Agency, "Kazakhstan – King Air B300ER Scorpion Aircraft with Intelligence, Surveillance, Reconnaissance (ISR) Mission Systems," transmittal no. 21-09, December 23, 2020, https://www.dsca.mil/sites/default/files/mas/Press_Release-Kazakhstan_21-09_CN.pdf.

54 Eurasian Resources Group, "Group at a Glance," accessed December 29, 2024, https://www.eurasianresources.lu/en/pages/group-at-a-glance/group-at-a-glance.

55 Elena Safirova "The Mineral Industry of Kazakhstan," U.S. Geological Survey, December 2019, 24.2, https://pubs.usgs.gov/myb/vol3/2019/myb3-2019-kazakhstan.pdf.

56 U.S. Department of State, "U.S. Security Cooperation With Indonesia," March 23, 2021, https://www.state.gov/u-s-security-cooperation-with-indonesia.

57 MIND ID, "About U.S. ," accessed December 29, 2024, https://mind.id/en/pages/tentang-kami.

58 Eurasian Resources Group, "Group at a Glance," accessed December 29, 2024, https://www.eurasianresources.lu/en/pages/group-at-a-glance/group-at-a-glance.

59 U.S. Department of State, "Minerals Security Partnership (MSP): Principles for Responsible Critical Mineral Supply Chains," February 2023, https://www.state.gov/wp-content/uploads/2023/02/MSP-Principles-for-Responsible-Critical-Mineral-Supply-Chains-Accessible.pdf.

60 "Fiscal Year 2018 Sales Total $55.66 Billion," Defense Security Cooperation Agency, October 9, 2018, https://www.dsca.mil/news-media/news-archive/fiscal-year-2018-sales-total-5566-billion; and The President, "Executive Order 13817 of December 20, 2017: A Federal Strategy To Ensure Secure and Reliable Supplies of Critical Minerals," Federal Register 82, no. 246 (December 26, 2017): 60835–60837, https://www.govinfo.gov/content/pkg/FR-2017-12-26/pdf/2017-27899.pdf.

61 For the criteria list to assess eligibility for foreign military sales, see Defense Security Cooperation Agency, Security Assistance Management Manual, C4.1. - Who May Purchase Using the FMS Program, https://samm.dsca.mil/chapter/chapter-4#C4.1. For a list of potential purchasers and their eligibility for foreign military sales, see Defense Security Cooperation Agency, Security Cooperation Customer and Regional Codes and FMS Eligibility Tables, Table C4. 1. 2. All Entries, https://samm.dsca.mil/table/table-c4t2all.

62 22 U.S.C. §2403(d)(1)–(4), https://uscode.house.gov/view.xhtml?req=(title:22%20section:2403%20edition:prelim). "Defense article" is defined as
"(1) any weapon, weapons system, munition, aircraft, vessel, boat or other implement of war;
(2) any property, installation, commodity, material, equipment, supply, or goods used for the purposes of furnishing military assistance;
(3) any machinery, facility, tool, material supply, or other item necessary for the manufacture, production, processing repair, servicing, storage, construction, transportation, operation, or use of any article listed in this subsection; or

(4) any component or part of any article listed in this subsection; but shall not include merchant vessels or, as defined by the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011), source material (except uranium depleted in the isotope 235 which is incorporated in defense articles solely to take advantage of high density or pyrophoric characteristics unrelated to radioactivity), by-product material, special nuclear material, production facilities, utilization facilities, or atomic weapons or articles involving Restricted Data."

63 Foreign Assistance Act of 1961, Public Law 118–83 (1961): 1–275, https://www.govinfo.gov/content/pkg/COMPS-1071/pdf/COMPS-1071.pdf.

64 An Act to Amend the Foreign Assistance Act of 1961 and the Foreign Military Sales Act, and for Other Purposes, Public Law 94–329, U.S. Statutes at Large 90 (1976): 729–769, https://www.govinfo.gov/content/pkg/STATUTE-90/pdf/STATUTE-90-Pg729.pdf.

65 Christina L. Arabia, Nathan J. Lucas, and Michael J. Vassalotti, "Transfer of Defense Articles: U.S. Sale and Export of U.S.-Made Arms to Foreign Entities," R46337, Congressional Research Service, updated March 23, 2023, 1, https://crsreports.congress.gov/product/pdf/R/R46337/4.

66 William E. Landay III, "Reissuance of the Security Assistance Management Manual (SAMM) as Defense Security Cooperation Agency (DSCA) Manual 5105.38-M, DSCA Policy 12-20," Defense Security Cooperation Agency, April 30, 2012, https://samm.dsca.mil/listing/authorization-letter.

67 Under the Arms Export Control Act (AECA), Congress requires notification for significant FMS transactions. Specifically, the President must formally notify Congress 30 calendar days before concluding a government-to-government foreign military sale if the transaction involves: Major defense equipment valued at $14 million or more; defense articles or services valued at $50 million or more; and design and construction services valued at $200 million or more. See

68 Christina L. Arabia, Nathan J. Lucas, and Michael J. Vassalotti, "Transfer of Defense Articles: U.S. Sale and Export of U.S.-Made Arms to Foreign Entities," R46337, Congressional Research Service, updated March 23, 2023, 4, https://crsreports.congress.gov/product/pdf/R/R46337/4.

69 C. Todd Lopez, "A Year in, DOD Racks Up Wins for Foreign Military Sales," U.S. Department of Defense, August 8, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3866263/a-year-in-dod-racks-up-wins-for-foreign-military-sales/.

70 C. Todd Lopez, "A Year in, DOD Racks Up Wins for Foreign Military Sales," U.S. Department of Defense, August 8, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3866263/a-year-in-dod-racks-up-wins-for-foreign-military-sales/.

71 Defense Security Cooperation Agency, "India – MK 54 MOD 0 Lightweight Torpedoes," transmittal no. 24-101, October 7, 2024, https://www.dsca.mil/sites/default/files/mas/Press%20Release%20-%20India%2024-101%20CN.pdf.

72 Defense Security Cooperation Agency, "Italy – Electronic Attack Mission System," transmittal no. 24-98, October 7, 2024, https://www.dsca.mil/sites/default/files/mas/Press%20Release%20-%20Italy%2024-98%20CN.pdf.

73 Defense Security Cooperation Agency, "Romania – Sentinel Radar Systems," transmittal no. 24-109, October 7, 2024, https://www.dsca.mil/sites/default/files/mas/Press%20Release%20-%20Romania%2024-109%20CN.pdf.

74 Defense Security Cooperation Agency, "Kingdom of Saudi Arabia – AGM-114R3 Hellfire II Missiles," transmittal no. 20-62, October 11, 2024, https://www.dsca.mil/sites/default/files/mas/Press%20Release%20-%20Kingdom%20of%20Saudi%20Arabia%2020-62%20CN.pdf; Defense Security Cooperation Agency, "Kingdom of Saudi Arabia – AIM-9X Block II Sidewinder Missiles," transmittal no. 24-46, October 11, 2024, https://www.dsca.mil/sites/default/files/mas/Press%20Release%20-%20Kingdom%20of%20Saudi%20Arabia%2024-46.pdf; and Defense Security Cooperation Agency, "Kingdom of Saudi Arabia – Ammunition for Artillery Systems, Machine Guns, and Tanks," transmittal no. 21-15, October 11, 2024, https://www.dsca.mil/sites/default/files/mas/Press%20Release%20-%20Kingdom%20of%20Saudi%20Arabia%2021-15%20CN.pdf.

75 Defense Security Cooperation Agency, "United Arab Emirates – GMLRS and ATACMS Munitions," transmittal no. 20-79, October 11, 2024, https://www.dsca.mil/sites/default/files/mas/Press%20Release%20-%20UAE%2020-79%20CN.pdf.

76 Defense Security Cooperation Agency, Security Assistance Management Manual, Table C5.T2. IAs Authorized to Receive Letters of Request, https://samm.dsca.mil/table/table-c5t2.

77 For example, the first Trump Administration's Conventional Arms Transfer policy stated, "When a proposed transfer is in the national security interest, which includes our economic security, and in our foreign policy interest, the executive branch will advocate strongly on behalf of United States companies." See Donald J. Trump, "National Security Presidential Memorandum Regarding U.S. Conventional Arms Transfer Policy," April 19, 2018, https://trumpwhitehouse.archives.gov/presidential-actions/national-security-presidential-memorandum-regarding-u-s-conventional-arms-transfer-policy/.

78 White House, "Remarks by President Trump and Crown Prince Mohammed Bin Salman of the Kingdom of Saudi Arabia Before Bilateral Meeting," March 20, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-crown-prince-mohammed-bin-salman-kingdom-saudi-arabia-bilateral-meeting/.

79 Defense Security Cooperation Agency, "Israel – 155mm Artillery Ammunition," transmittal no. 24-16, December 29, 2023, https://www.dsca.mil/sites/default/files/mas/Press%20Release%20-%20Israel%2024-16%20CN.pdf; and John Hudson and Mikhail Klimentov, "U.S. Approves $147.5 Million Sale of Artillery Ammunition and Gear to Israel," Washington Post, December 30, 2023, https://www.washingtonpost.com/national-security/2023/12/30/us-weapons-sale-israel-blinken/.

80 "Security Cooperation Overview," Defense Security Cooperation Agency, accessed December 31, 2024, https://www.dsca.mil/foreign-customer-guide/security-cooperation-overview.

81 According to 50 U.S.C. §4533, "To create, maintain, protect, expand, or restore domestic industrial base capabilities essential for the national defense, the President may make provision or purchases of or commitments to purchase an industrial resource or a critical technology item, for Government use or resale. See 50 U.S.C. §4533(a)(1)(A), https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AU.S. C-prelim-title50-section4533&num=0&saved=%7CKHRpdGxlOjUwIHNlY3Rpb246NDUzMyBlZGl0aW9uOnByZWxpbSk%3D%7C%7C%7C0%7Cfalse%7Cprelim.

82 According to 50 U.S.C. §4533(b), "Subject to the limitations in subsection (a), purchases and commitments to purchase and sales under subsection (a) may be made without regard to the limitations of existing law (other than section 1341 of title 31), for such quantities, and on such terms and conditions, including advance payments, and for such periods, but not extending beyond a date that is not more than 10 years from the date on which such purchase, purchase commitment, or sale was initially made, as the President deems necessary, except that purchases or commitments to purchase involving higher than established ceiling prices (or if no such established ceiling prices exist, currently prevailing market prices) or anticipated loss on resale shall not be made, unless it is determined that supply of the materials could not be effectively increased at lower prices or on terms more favorable to the Government, or that such purchases are necessary to assure the availability to the United States of overseas supplies." See 50 U.S.C. §4533(b), https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AU.S. C-prelim-title50-section4533&num=0&saved=%7CKHRpdGxlOjUwIHNlY3Rpb246NDUzMyBlZGl0aW9uOnByZWxpbSk%3D%7C%7C%7C0%7Cfalse%7Cprelim.

83 50 U.S.C. §4517(b)(2), https://uscode.house.gov/view.xhtml?req=(title:50%20section:4517%20edition:prelim).

84 For example, if the Department of Defense has right-of-first-refusal for 5,000 metric tons of antimony metal and oxide, and Defense Firms A, B, and C collectively request 7,000 metric tons, the Department of Defense needs a process to allocate these minerals.

85 Joseph R. Biden, Jr., "Memorandum on Presidential Waiver of Statutory Requirements Pursuant to Section 303 of the Defense Production Act of 1950, as amended, on Department of Defense Supply Chains Resilience," February 27, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/27/memorandum-on-presidential-waiver-of-statutory-requirements-pursuant-to-section-303-of-the-defense-production-act-of-1950-as-amended-on-department-of-defense-supply-chains-resilience/; and 50 U.S.C. §4533, https://uscode.house.gov/view.xhtml?req=(title:50%20section:4533%20edition:prelim).

86 Joseph R. Biden, Jr., "Memorandum on United States Conventional Arms Transfer Policy," February 23, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/23/memorandum-on-united-states-conventional-arms-transfer-policy/.

87 Defense Security Cooperation Agency, Security Assistance Management Manual, C4.3.5.3., https://samm.dsca.mil/chapter/chapter-4#C4.3. The State Department could make this determination based on the criterion of considering the "United States Political-Military Relationship with the End User." Additionally, some defense articles are already designated as FMS-Only, so FMS may already be required for the requested defense articles. See Defense Security Cooperation Agency, Security Assistance Management Manual, C4.3.5.4.1., C4.3.5.2, https://samm.dsca.mil/chapter/chapter-4#C4.3; and J. W. Rixey, "Revision of Security Assistance Management Manual Chapter 4 Regarding Foreign Military Sales-Only Designations, DSCA Policy 16-51 [SAMM E- Change 325]," Defense Security Cooperation Agency, December 5, 2016, https://samm.dsca.mil/sites/default/files/DSCA%2016-51.pdf.

88 22 U.S.C. §2301, https://uscode.house.gov/view.xhtml?path=/prelim@title22/chapter32/subchapter2&edition=prelim.

89 22 U.S.C. §2751, https://uscode.house.gov/view.xhtml?req=42+u.s.c.+2751-.

90 Evidence that strengthening U.S. mineral supply chains is now part of U.S. foreign policy includes executive orders from both President Donald Trump and President Joseph Biden. See The President, "A Federal Strategy To Ensure Secure and Reliable Supplies of Critical Minerals," Executive Order 13817, Federal Register 82, no. 246 (December 26, 2017): 60835–60837, https://www.govinfo.gov/content/pkg/FR-2017-12-26/pdf/2017-27899.pdf; and The President, "America's Supply Chains," Federal Register 86, no. 38 (March 1, 2021): 11849–11854, https://www.govinfo.gov/content/pkg/FR-2021-03-01/pdf/2021-04280.pdf.

91 22 U.S.C. §2751, https://uscode.house.gov/view.xhtml?req=42+u.s.c.+2751-.

92 Joseph R. Biden, Jr., "Memorandum on United States Conventional Arms Transfer Policy," February 23, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/23/memorandum-on-united-states-conventional-arms-transfer-policy/.

93 Donald J. Trump, "National Security Presidential Memorandum Regarding U.S. Conventional Arms Transfer Policy," April 19, 2018, https://trumpwhitehouse.archives.gov/presidential-actions/national-security-presidential-memorandum-regarding-u-s-conventional-arms-transfer-policy/.

94 Jahara Matisek and Ivor Wiltenburg, "Security Force Assistance as a Preferred Form of 21st Century Warfare: The Unconventional Becomes the Conventional," in The Conduct of War in the 21st Century, ed. Rob Johnson, Martijn Kitzen, and Tim Sweijs (New York: Routledge, 2021): 173–188, https://www.taylorfrancis.com/chapters/edit/10.4324/9781003054269-16/security-force-assistance-preferred-form-21st-century-warfare-jahara-matisek-ivor-wiltenburg.

95 Jahara Matisek, "International Competition to Provide Security Force Assistance in Africa: Civil-Military Relations Matter," PRISM 9, no. 1 (2020): 103–113, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_103-113_Matisek%203.pdf?ver=v4ykp2L-6tGx1-DrkQcrAQ%3d%3d.

96 Institute for Defense Analyses, "Key Materials for High-Priority Weapon Systems, and Assessing Risks to Their Supply: A Report for the U.S. Defense National Stockpile Center," July 31, 2008, in U.S. Department of Defense, "Reconfiguration of the National Defense Stockpile Report to Congress," April 2009, B-2, https://www.scribd.com/document/16483302/Reconfiguration-of-the-National-Defense-Stockpile-Report-to-Congress.

97 Chad A. Friedline, "Tin," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 184, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-tin.pdf.

98 Cameron M. Keys, "Emergency Access to Strategic and Critical Materials: The National Defense Stockpile," R47833, Congressional Research Service, November 14, 2023, 44, https://crsreports.congress.gov/product/pdf/R/R47833.

99 Chad A. Friedline, "Tin," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 184, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-tin.pdf.

100 Chad A. Friedline, "Tin," in U.S. Geological Survey, Mineral Commodity Summaries 2024 (Reston, VA: U.S. Geological Survey, 2024), 184, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-tin.pdf.

101 In 2021, Indonesia mined and smelted an estimated 70,000 metric tons of tin. See U.S. Geological Survey, "Advance Data Release of the 2020–21 Annual Tables," Indonesia, Table 1, accessed December 29, 2024, https://www.usgs.gov/centers/national-minerals-information-center/asia-and-pacific.

102 In 2023, PT Timah Tbk produced an estimated 15,340 metric tons of tin. The Indonesian government (MIND ID) has 65% ownership in PT Timah Tbk, while the public has 35% ownership. See PT Timah Tbk, "Annual Report," 2023, 52, 139, https://timah.com/userfiles/post/240429662F51E4380C3.pdf.

103 Defense Security Cooperation Agency, "Indonesia – F-15ID Aircraft," transmittal no. 22-13, February 10, 2022, https://www.dsca.mil/sites/default/files/mas/Press%20Release%20-%20Indonesia%2022-13%20CN.pdf.

104 Defense Security Cooperation Agency, "Indonesia – MV-22 Block C Osprey Aircraft," transmittal no. 20-27, July 6, 2020, https://www.dsca.mil/sites/default/files/mas/indonesia_20-27.pdf.

105 Defense Security Cooperation Agency, "Indonesia-AIM-120C-7 Advanced Medium-Range Air-to-Air Missiles (AMRAAMs)," transmittal no. 15-81, March 10, 2016, https://www.dsca.mil/sites/default/files/mas/indonesia_15-81.pdf.

106 Defense Security Cooperation Agency, "Indonesia – AIM-9X-2 Sidewinder Missiles," transmittal no. 15-28, May 5, 2015, https://www.dsca.mil/sites/default/files/mas/indonesia_15-28_0.pdf.

107 Donald J. Trump, "National Security Presidential Memorandum Regarding U.S. Conventional Arms Transfer Policy," April 19, 2018, https://trumpwhitehouse.archives.gov/presidential-actions/national-security-presidential-memorandum-regarding-u-s-conventional-arms-transfer-policy/.

108 For an example of an Integrated Country Strategy, see U.S. Department of State, "Integrated Country Strategy: India," approved May 27, 2022, https://www.state.gov/wp-content/uploads/2022/07/ICS_SCA_India_Public.pdf.

109 U.S. Department of State, "Integrated Country Strategies," accessed December 29, 2024, https://www.state.gov/integrated-country-strategies/; and Christina L. Arabia, Nathan J. Lucas, and Michael J. Vassalotti, "Transfer of Defense Articles: U.S. Sale and Export of U.S.-Made Arms to Foreign Entities," R46337, Congressional Research Service, updated March 23, 2023, 21, https://crsreports.congress.gov/product/pdf/R/R46337/4.

CEO of Scale A.I. Alexandr Wang, American Enterprise Institute fellow Klon Kitchen, and Global A.I. ethicist at DataRobot Dr. Haniyeh Mahmoudian testify during a House Armed Services Subcommittee on Cyber, Information Technologies and Innovation hearing about artificial intelligence on Capitol Hill July 18, 2023, in Washington, D.C. (Drew Angerer / Getty Images)

Targeted and Precise: Innovation Versus Regulation in the Critical Technology Sector

Courtney Manning

Introduction: The U.S. Critical Technology Ecosystem

Despite popular media portrayals of self-taught entrepreneurs developing technological marvels in rented garages, new innovations in the United States are predominantly funded and sustained through federal initiatives bolstering successful enterprises. The strengthening bond between technology giants and Washington over time is a function of the centrality of cutting-edge tech to two areas vital to the national interest in the 21st century: military-technological supremacy and economic competition with China.

For the U.S. Department of Defense, the value added by public-private cooperation is self-evident: Leadership in advanced technologies deters and provides an asymmetric advantage against U.S. adversaries, and for the past 40 years, nearly all groundbreaking innovations have originated from domestic private firms. Procuring and outsourcing cutting-edge products and services strengthens the

defense-industrial base at a fraction of the cost of equivalent public-sector projects while expanding American geopolitical influence and bolstering gross domestic product (GDP). In return, the Department of Defense serves as a "venture customer" that provides substantial funding – at substantial financial risk – for private-sector innovations before consumer demand rises to fill the gap.[1]

For the executive branch, at least in peacetime, ensuring that the United States remains a global hegemon takes primacy. After securing international dominance in manufacturing by the end of World War II, America kept its lead by localizing high-value, low-hazard activities like research and development (R&D) and outsourcing low-value, labor-intensive tasks like mining and manufacturing to countries in the Global South.[2] Prioritizing operations higher on global value chains allowed American technology firms to increase profitability without significant public investment or regulatory intervention.[3] Instead, free trade, foreign partnerships, and strategic global investments enabled the United States to surpass the technological capacities of all other countries in the system and attract new ideas and investment into its orbit.

Decades of laissez-faire oversight and unregulated capital consolidation, however, gradually whittled down America's innovation dynamism. U.S. leadership in sourcing and production slowed, driving depreciating returns in economic growth and productivity across all but a few geographic areas and specialties.[4] Ensuring local diversity of outputs beyond R&D was critical for market disruption, but the infrastructure required to support activities like manufacturing and after-sales service no longer existed domestically. As policymakers grappled with this new reality, a nation that had spent the past quarter-century testing radical industrial policies began challenging the foundational principles of the U.S. free-market system: the People's Republic of China (PRC).

By securing near-monopolies over several non-R&D activities and investing $912 billion in technology start-ups between 2013 and 2023, China gained unprecedented leverage over global technology markets.[5] Aggressive state-driven investment, mercantilist industrial policies, and exploitation of free market and innovation ecosystems soon began to drive rapid advances in artificial intelligence (AI), quantum sensors, electric batteries, and advanced manufacturing.[6] Despite Western assertions that these strategies would fail to drive indigenous research and development,[7] China soon surpassed the U.S. in several key AI metrics, including number of patents filed,[8] research papers published,[9] and public investment as a share of GDP.[10]

Despite these risks, the importance of sustaining America's technological hegemony can seem distant from the interests of the average taxpayer. Developing bleeding-edge technologies requires billions of dollars and years of sustained funding for geopolitical advantages that may never materialize. In a politically polarized nation where kitchen-table economics increasingly supersedes abstract technocratic objectives,[11] sustaining public support for broad industrial initiatives across multiple election cycles poses a significant challenge – one that single-party states like China are not constrained by.

Enter public diplomacy and political advocacy. While only four in 10 Americans believe that the People's Republic of China's technological capacity is "of very serious concern," its human rights record, support for Russia, and tensions with Taiwan represent more salient threats in the public lexicon.[12] To sustain bipartisan and public support for the policies needed to stay ahead of Beijing, Washington must frame U.S.-China strategic competition as an ideological war, with democratic values and ethics on one side and authoritarianism and territorial encroachment on the other.

While this portrayal is conceptual, the underlying risks are real. By funneling innovations from its private sector and foreign collaborators into its military apparatus, the Chinese Communist Party aims to "intelligentize" its People's Liberation Army (PLA) and supersede the United States in next-generation warfare by 2035.[13] The Australian Strategic Policy Institute finds that while U.S. firms dominate in commercial AI sales, China's leadership in 24 technologies with a high risk of monopoly includes every single one with defense applications.[14] If China's autonomous drone systems, cyber warfare tools, and advanced missile technologies surpass U.S. capabilities, it could not

only undermine American technological leadership but also shift the global balance of power and sideline the liberal, rules-based order that has long underpinned U.S. foreign policy. For this reason, preventing innovation stagnation is not a hypothetical or distant concern – it is a direct threat to U.S. national security, economic stability, and global influence, and as such requires unprecedented government intervention.

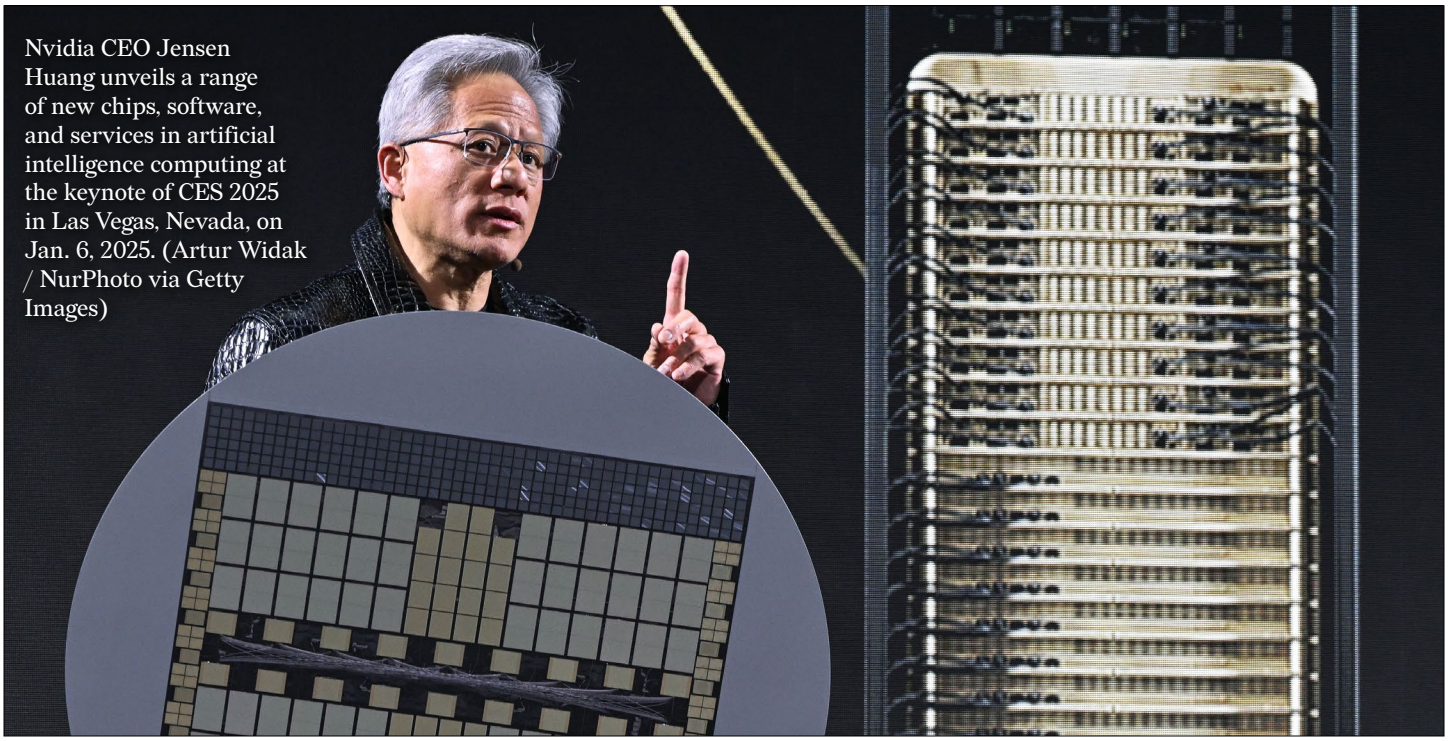
Industrial Policy Goals and Mechanisms

U.S. critical technology initiatives may not inhibit China's economic development, alter its territorial claims, or mitigate its authoritarianism, but within an economic competitiveness framework, none are necessary to "beat China." Rather, the U.S. "winning" the global technology race comprises gaining dominance over a range of strategic investments that pay dividends in both conflict and peacetime, and then using those investments for public good at home and to promote U.S. influence abroad. The more resources that are applied to this effort (and to building strong coalitions that multiply gains and protect shared spoils), the more China is deterred from future geopolitical malfeasance and incentivized to follow the rules-based liberal order.

Within this strategic competition framework, a successful industrial policy strategy for critical technology development (1) maximizes national return on investment, (2) aligns the ensuing benefits with the public interest, (3) mitigates the risk of exploitation by adversaries, and (4) furthers U.S. foreign policy goals. Legislators must ensure these needs are met while providing sufficient incentives for firms to cooperate with – and even promote – regulations that affect their bottom line.

Allocation and Coordination of National Resources

The first priority for U.S. industrial policy is to maximize national return on investment, either directly through revenue generation or indirectly through benefits to society and national security. Corporate taxes on the technology sector redistribute the disproportionately high financial returns of a small group of innovators across broad spending buckets like health care, infrastructure, and education. Targeted fiscal mechanisms – such as subsidies, public-private partnerships, and tax incentives – reinvest those revenues back into the innovation ecosystem.[15]



Nvidia CEO Jensen Huang unveils a range of new chips, software, and services in artificial intelligence computing at the keynote of CES 2025 in Las Vegas, Nevada, on Jan. 6, 2025. (Artur Widak / NurPhoto via Getty Images)

American corporate tax rates are substantially lower than in other developed countries, bringing in less revenue as a share of GDP than nearly all other market-based economies.[16] As a result, the United States spends less on R&D as a percentage of its GDP than Israel and South Korea.[17] In 2024, the Biden administration budgeted $209 billion for public science and technology programs,[18] including $102 billion for health and social equity initiatives.[19] China currently spends about five times more on its supply-side investments,[20] funneling more than $912 billion into critical technology startups alone over the past 10 years.[21] However, substantial tax credits and subsidies make private sector R&D more lucrative in the United States than in China. As Washington's spending on R&D as a function of GDP has declined,[22] total U.S. investment in research and development has increased exponentially, with corporate spending now comprising nearly 80% of the U.S. total.[23]

Private sector R&D expenditures result in more cost-effective and market-oriented innovations than are typically produced by the public sector. However, capital investment alone does not inherently drive output of new technologies.[24] Functional constraints, including specialized labor, raw materials, machinery, and research time, become more burdensome as demand for cutting-edge tech expands. The critical technology sector must also make investments to protect its proprietary technology, data, and supply chains from extortion and theft.[25] Well-resourced firms that are unable or unwilling to address these systemic challenges tend to redirect new capital into areas with fewer constraints, such as stock buybacks and executive salaries.[26] The resulting rentiership and bureaucratic bloat drive diminishing returns that weaken return on investment as additional resources are injected.

For this reason, Washington must invest not only in individual firms but also in the foundational infrastructure underpinning the critical technology sector. Energy grids, data networks, and transportation lines must be robust for emerging technology initiatives to be effective.[27] Over time, the responsibilities of labor provision, job training, and benefits like retirement and health insurance have also shifted from the private to the public sector due to the former's exponential growth model and the latter's accelerating demand for dual-use technologies.[28] In semiconductor manufacturing, for instance, federal and state job training programs allow firms to improve total factor productivity by increasing their hiring requirements rather than provide on-the-job instruction, though the Semiconductor Industry Association projects that 58% of new jobs will go unfilled by 2030 without significant program expansion.[29, 30]

As federal responsibilities expand, investments in coordination, administration, and oversight must rise in tandem. Starting with President Donald Trump's "Executive Order on Maintaining American Leadership in Artificial Intelligence" in 2019,[31] executive orders became the primary vehicle to authorize new administrative capacity. Subsequent orders reformed the Cybersecurity and Infrastructure Security Agency and bolstered existing export mechanisms such as the Bureau of Industry and Security (BIS), Committee on Foreign Investment in the United States (CFIUS), and Office of Foreign Assets Control (OFAC). President Joe Biden continued his predecessor's focus on strategic technologies but emphasized multisector applications such as infrastructure, health, and social equity. Biden signed into law the Infrastructure Investment and Jobs Act, the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act, and the Inflation Reduction Act. These new and expanded vehicles oversee more than 160 new R&D programs with more than $730 billion in funding.[32] Finally, National Defense Authorization Acts allow Congress to regulate innovation, with the 2021 law establishing the National Artificial Intelligence Initiative Office and the 2023 law banning Chinese semiconductors from government contractor supply chains.[33, 34]

Domestic Regulations and Award Conditions

Improved access to infrastructure, labor, and capital lowers the cost of entry for new players in the advanced technology space, increasing innovation dynamism and GDP. However, net benefits to the U.S. economy do not always represent net benefits to the average American. The cultural communication supporting these enormous investments is undermined if Washington's priorities are unable to be sufficiently differentiated from those of the Chinese Communist Party or other unsavory regimes. If U.S. citizens feel unjustly surveilled, overtaxed, underpaid,

or politically disenfranchised due to federally funded advancements in emerging technologies, public support for these initiatives will decline. For the government , this means losing not only the potential economic benefits of an innovation but also the geopolitical and military advantages it provides.

Legislation, regulations, and grant terms ensure that Washington's critical technology investments reflect American ethics and values. Principles like social equity, privacy, human rights, and democracy are not inherent to free markets; on the contrary, when left unchecked, emerging technologies tend to serve the interests of capital-rich investors over unmet social needs.[35] Executive orders and memorandums, like the Biden administration's Policy to Advance Governance, Innovation, and Risk Management in Federal Agencies' Use of AI, aim to predict and prevent negative externalities that could arise from new technology investments.[36] Program regulations and grant agreements, like the CHIPS and Science Act's requirement that firms seeking $150 million in funding provide childcare plans for their blue-collar workforce, ensure that taxpayer-funded programs contribute to the public good.[37]

Trade and Export Controls

Export, investment, and trade controls aim to prevent bad actors from unduly exploiting America's innovations and international collaborations, gain an asymmetric advantage over the state, or pose threats to U.S. national security. Trade policy determines what products, services, and end users are of particular importance to U.S. global leadership and defense, while Export Administration Regulations (EARs) ensure that these assets are protected from exploitation and capture by foreign adversaries.

The primary authorizing statutes for export controls are the Arms Export Control Act, the Export Control Reform Act, and the International Emergency Economic Powers Act. With executive branch coordination from the Office of the U.S. Trade Representative,[38] oversight and enforcement of U.S. export controls are dispersed across several government agencies. If a foreign entity is deemed to threaten U.S. national security, OFAC and BIS place it on one or more end-user sanctions lists with varying degrees of restrictions.[39] Export controls for all commercial items – as well as many dual-use

Key fobs are produced at a manufacturing plant in Tlajomulco de Zuniga, Jalisco State, Mexico, on Feb. 20, 2025. (Ulises Ruiz / AFP via Getty Images)

technologies such as semiconductors, AI, and quantum computers – are also enforced by BIS.[40] Export controls for conventional weapons and other dual-use technologies, meanwhile, are directed by the State Department's Conventional Arms Threat Reduction Office.[41] The International Traffic in Arms Regulations, a section of the Arms Export Control Act, grants the State Department's Directorate of Defense Trade Controls jurisdiction over munitions and defense articles and services not covered by other entities.[42]

While export controls help ensure that U.S. products and services are unable to reach America's adversaries, import controls like taxes, tariffs, and duties are used to offset injurious trade practices and gain leverage in international negotiations. The president is granted broad authority by Congress to impose tariffs and duties on imports that threaten U.S. security or the national interest.[43] The secretary of the treasury then interprets these orders and drafts regulations to be enforced by U.S. Customs and Border Protection at U.S. ports of entry.

A final set of policies ensure that nonsensitive products and services are diffused fairly throughout the international environment. Section 301 of the U.S. Trade Act authorizes the president to impose tariffs and other trade restrictions on countries that unduly burden or restrict free trade, regardless of their membership in the World Trade Organization (WTO).[44] This authority gained prominence in 2018, when Trump imposed a series of tariffs to pressure the Chinese government to rescind its policies and practices related to technology transfer and intellectual property theft.[45] Before this, these activities faced few unilateral repercussions from other countries, with WTO cases and patent infringement lawsuits providing the primary mechanisms for dispute resolution. Afterward, several nations – including non-European countries like India and Vietnam – followed the United States' lead in imposing tariffs on China's technology industries.[46]

Foreign Investment and Transaction Controls

In addition to ensuring that its exports do not increase risks to national security, the United States aims to monitor and prevent innovations deemed "critical" or "dual use" from being acquired or invested in by its competitors and adversaries. In 1975, President Gerald Ford's Executive Order 11858 established CFIUS to prevent foreign firms from capturing the uppermost benefits from the U.S. critical technology and defense sector.[47] The primary statutes authorizing CFIUS are the Defense Production Act of 1950, the Foreign Investment Risk Review Modernization Act of 2018, and the Foreign Investment and National Security Act of 2007.[48] Over time, CFIUS's oversight has expanded from reviewing foreign mergers and acquisitions of U.S. companies that are integral to defense supply chains to overseeing a wide variety of transactions, mergers, and noncontrolling investments in critical industries as well as real estate near military and maritime installations.

Inverse mechanisms prevent U.S. firms from investing in or acquiring foreign assets that might be used against the country or its sensitive industries. While U.S. partners such as Japan, Taiwan, and South Korea have long maintained restrictions on outbound investment in foreign dual-use technologies, U.S. tech firms have had broad agency to partner with foreign entities on advanced research centers, fabrication plants, and joint ventures. While CFIUS is not authorized to oversee these transactions, mechanisms have recently been instituted to monitor and prevent PRC military and intelligence agencies from benefiting from them.[49] These include the CHIPS and Science Act's requirement that grantees not expand manufacturing in China for at least 10 years and the U.S. Outbound Investment Security Program's prohibition of outbound investments in a number of Chinese industries.[50] This departure from traditional U.S. policy aims to be limited in scope to only specified products and firms associated with PRC military and intelligence activities. However, Beijing's expansive civil-military fusion regime and Washington's decentralized and overlapping regulatory structure make enforcement of these policies extraordinarily difficult, particularly when they require investigations of foreign subsidiaries and intermediaries in addition to U.S. investments and transactions.

Finally, domestic regulations on trade and investment are used to promote cosmopolitan foreign policy objectives, such as reducing forced labor and corruption abroad. BIS is broadly required to consider human rights concerns when reviewing trade license applications, and it must reject specific products and

services when directed by the president and other authorities under part 766 of the EAR.[51] For example, BIS is required to deny export licensing for products and services used by the PRC for crime control and surveillance in Hong Kong.[52] Additionally, statutes such as the Uyghur Forced Labor Prevention Act[53] and Global Magnitsky Act[54] prevent U.S. entities from engaging in trade with foreign entities responsible for gross violations of internationally recognized human rights. As with part 766 orders, these prohibited end users and products of concern must first be stipulated by the president or another specified authority.

Cooperative Agreements and Regimes

The final objective of U.S. economic competition policy is to create foreign initiatives that sustain U.S. global leadership and influence. The most significant multilateral regimes regulate global proliferation of weapons of mass destruction and "destabilizing accumulations" of conventional weapons and dual-use technologies: the Wassenaar Arrangement, Nuclear Suppliers Group, Australia Group, and Missile Technology Control Regime.[55] The second-largest multilateral agreements are those that regulate free and fair trade. One of the most active international dispute settlement institutions in the world, the WTO, is dedicated to ensuring its signatories maintain open, fair, and undistorted economic competition policies and practices.[56] The World Bank, the United Nations Conference on Trade and Development, and the Organization for Economic Cooperation and Development also promote democratic and market economic principles; negotiations for the latter two mechanisms are overseen by the Office of the U.S. Trade Representative.

Policy considerations under trade agreements have become broader and more sophisticated over time. According to the United Nations Conference on Trade and Development, issues currently governed by regional trade agreements include environmental protection, migration, workplace safety, and intellectual property rights.[57] International mechanisms also

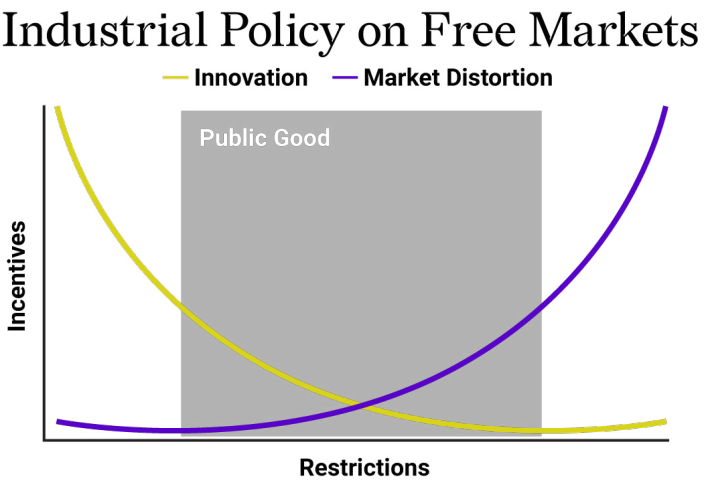
Federal Reserve Chair Jerome Powell testifies before the Senate Banking Committee about the Fed's continuing efforts to tame inflation and ease borrowing costs in the face of new tariffs, possible tax cuts, and other institutional moves by the Trump administration on Capitol Hill on Feb. 11, 2025, in Washington, D.C. (Chip Somodevilla / Getty Images)

govern trade in emerging technologies. Both the U.S.-EU Trade and Technology Council and the Export Controls and Human Rights Initiative research and publish international standards for exporting technologies that may be misused for human rights violations. Other mechanisms – such as the Indo-Pacific Economic Framework, Americas Partnership for Economic Prosperity, and International Technology Security and Innovation fund – promote resilient critical technology supply chains.[58]

Regulatory Risk in the Critical Technology Sector

In exchange for their contributions to the defense and public sectors, technology firms receive generous incentives that allow them to innovate broader and further than through private investment alone. As long as the government provides these incentives, it is able to influence which innovations are developed, where they should go, and who should use them. However, if Washington's web of policies and priorities becomes too prohibitive to navigate, firms will move elsewhere to secure ongoing shareholder returns. For this reason, industrial policy must ensure that a broad range of firms are incentivized to cooperate with the demands of federal and state agencies.

Because the U.S. is a democracy, equilibrium between the interests of firms and the government is not enough to justify large volumes of public spending. Both incentives and restrictions require public awareness and support, which is achieved by aligning initiatives with domestic priorities and ensuring sufficient tax revenue for other spending buckets. Industrial policies that infringe on free and fair trade have also traditionally required a credible national security justification to avoid unduly violating U.S. international agreements, making a minimum threshold of consent from U.S. partners and allies an unspoken requirement. However, recent shifts deprioritizing multilateralism in the executive branch have made this consideration less significant.



Source: Courtney Manning © 2025, The New Lines Institute for Strategy and Policy

The final major risk of industrial policy is market distortion. Even when incentives and restrictions are evenly balanced, industrial policies and other government interventions impose complex and unpredictable effects on the rest of the economic system.[59] For this reason, while a minimum level of regulation is needed to prevent exploitation by adversaries and rent-seeking firms, industrial policies should target only critical technologies with significant and understood military applications while maximizing agency for commercial innovators to collaborate and take risks. If not, the friction produced by colliding variables of successive waves of intervention will rapidly drive diminishing returns in innovation and technological development.

In periods of high market distortion, the technology sector is unable to efficiently meet the needs of the state and its citizens. Before the endpoint of complete isolationism or net-zero innovation, four gradually increasing negative effects provide warning signs that U.S. industrial policy is becoming too restrictive: protectionism, regulatory ambiguity, bureaucratic bloat, and escalation spirals.

Protectionism

The U.S. technology industry once cultivated a variety of economic activities, each providing continuous opportunities for innovation and market disruption. Eventually, prioritization of intellectual property creation – particularly hardware and software design – led to the offshoring of most other activities. Technology firms sacrificed long-term opportunities to innovate in processes like procurement, manufacturing, and after-sales service for immediate savings in labor costs. By 2019, intellectual property accounted for 41 percent of U.S. GDP and 44 percent of total U.S. employment,[60]

narrowing U.S. labor demand and creating high-risk supply chain dependencies.

To combat these risks, the first Trump administration proposed tariffs on manufactured goods and raw materials to reshore non-R&D activities, improve supply chain resiliency, and promote rural job creation. However, penalizing imports and foreign partnerships rarely motivates the creation of domestic replacement capacity.[61] A study by the Harvard Kennedy School determined that most U.S. companies affected by tariffs between 2018 and 2019 chose to downsize or move operations to the Indo-Pacific or Latin America rather than invest in domestic facilities.[62] Foreign partners are even more incentivized than domestic firms to move their operations elsewhere, significantly reducing U.S. tax revenue and employment.[63] Given that tariff collection accounts for only 1.57% of federal income as of 2024, federal enforcement costs and revenue losses far exceed revenue raised through new trade restrictions.[64]

While financial penalties can appear more cost effective than direct investment, the fiscal burden of policy implementation, enforcement, and oversight makes incentives more efficient in achieving short-term market change.[65] However, while initiatives like the CHIPS and Science Act can temporarily reinvigorate declining industries,[66] it is unlikely that these industries will be independently profitable without continued subsidies. Significant improvements in modernization and automation are needed to make critical technology manufacturing economically viable in the United States. Otherwise, reducing incentives or increasing subsidy requirements will lead firms to re-offshore or significantly increase product costs, causing ripple effects across upstream supply chains. This was demonstrated in 2023, when protectionist licensing restrictions and the Inflation Reduction Act's complicated subsidy restrictions led Ford Motor Company to cut investment and reduce hiring and production targets for its planned domestic battery projects.[67]

Domestic supply chain consolidation reduces economic efficiency and market diversity, slowing innovation and raising consumer prices. The PRC, which has spent decades attempting to drive rapid technological advancement with protectionism, faces significant and continuous hurdles in achieving a self-sustaining innovation ecosystem. When "foreign influence" was removed from the development process of China's COMAC C919 aircraft in 2008, the $70 billion public investment was delayed by nearly 10 years while replacement knowledge and infrastructure were built domestically. As of January 2025, the aircraft continues to fail certification and safety tests from aviation authorities outside China.[68, 69]

Finally, American isolationism encourages protectionist trade policies to spread across the international system. As tariffs rise between China and the U.S., some countries are lowering tariff rates to incentivize U.S. investment and manufacturing.[70] However, these cases are a minority, and many other countries – including Mexico, Vietnam, and South Africa – are raising duties on various links in the critical technology supply chain. Indonesia has ceased exporting some raw materials entirely, forcing foreign firms to process them onshore instead.[71] As countries with low tariffs and production costs tend to be less politically stable, investment and trade barriers between middle- and high-income partners become a prisoner's dilemma that drives investment to the bottom dollar rather than to improved supply chain security or strategic alignment.

Regulatory Ambiguity

Aligning critical technology development with the public interest requires significant accountability and oversight capacity. The broader the scope and desired impact of a given policy, the more funding is required to ensure that the policy meets its objectives. Because more complex technologies have more expansive supply chains, industrial controls in the U.S. critical technology sector must be targeted and precise to prevent regulations from becoming unwieldy, vague, and ultimately ineffective.

Broad regulations allow Beijing to demand proprietary technology and sensitive data from foreign entities in exchange for access to Chinese markets. By 2023, nearly 60% of surveyed U.S. businesses in the information technology industry stated they had considered closing or downsizing their Chinese operations due to the lack of clarity on key definitions in regulations.[72] According to a survey by the European

South Korean Foreign Minister Cho Tae-yul speaks during a press conference ahead of a U.N. Security Council meeting on the impacts of cyber threats on international peace and security at U.N. headquarters on June 20, 2024, in New York. (Yuki Iwamura / AFP via Getty Images)

Chamber of Commerce, "as the scope of 'important data' in [Chinese regulations] is yet to be defined by the National Financial Regulatory Administration, it makes it difficult for companies to determine which data must pass a security assessment [and] predict how stringent security assessment requirements will be."[73] The survey showed that European firms' decisions to downsize or reassess participation in Chinese markets primarily resulted from China's ambiguity in its policies and practices and not U.S. or EU industrial policies. The enormous profit potential of Chinese markets, however, means that years of recurring data breaches and escalating warnings from Western governments have mostly failed to slow trade and investment in China.

Unlike in China, where industrial policy mechanisms have been institutionalized for over a generation, the U.S. government was not designed to enforce broad trade restrictions and remains ill-equipped to do so.[74] Though China's regulatory ambiguity is intentional rather than the result of a decentralized regulatory structure, the result of broad trade policies in the United States is the same: reduced trade and investor confidence, and increased scrutiny from free trade partners and institutions. Some of these risks would subside if Washington was committed to comprehensively implementing and enforcing trade controls. However, because complete and nondiscriminatory enforcement of current controls would significantly undermine U.S. economic competitiveness, ambiguity is unlikely to decrease over the next four years.

Vendor Lock-In

Working with national champions in the critical technology industry provides Washington with several advantages in capacity, immediacy, and security. However, centralizing the assets and foundational resources of the emerging tech market in the hands of a few large companies risks homogenizing the foundational infrastructure underpinning the critical technology industry, making it difficult or impossible to maintain a competitive innovation landscape.

Additionally, "locking in" governments to commercial infrastructures, products, and services creates significant vulnerabilities that closed-system adversaries and competitors can exploit. When U.S. federal agencies use the same digital infrastructure as billions of global consumers, any individual or group with sufficient knowledge of that infrastructure's

weaknesses can access sensitive U.S. data and technology. Exploits in one agency's cyber defenses can grant hackers access to all other agencies in the system, magnifying potential harm. This was illustrated during the 2023 SolarWinds hack, when nearly two dozen high-profile U.S. government agencies were penetrated using the same entry procedures.[75]

Advocates of the national champions model posit that America's leading technology firms are also its leading cybersecurity firms, while smaller competitors are less capable of both providing services and protecting those services from predation. However, continuous awareness of new cyber threats and ongoing replacement of vulnerable code is extremely cost-intensive, especially for poorly maintained and aging systems that no longer bring in revenue. As a result, older and larger firms must sacrifice either profitability or security, and their obligation to shareholders often takes priority. To retain tech giants as providers, the government must pay not only for its own specialized services and security but also for the ongoing protection of the firm's substantial foreign and aging digital infrastructure. These investments can be prohibitive, but cutting costs magnifies cyber risk. In the case of the SolarWinds hack, detection and attribution were impossible because federal agencies used a cheaper software model without basic network security protections.

Several proposals have been made to force large technology firms to improve their cybersecurity practices.[76] However, the limited competition for service provision in cloud computing and other critical technology services skews the power dynamics between firms and the government, making these regulations unlikely to pass without proportionate financial assistance from Washington.[77] As a result, frameworks like the Office of Management and Budget's Federal Zero Trust Strategy place the burden of responsibility for cybersecurity on the end user and federal agencies instead of on providers.[78] While strengthening public-sector cybersecurity expertise is important, stringent government contract agreement clauses protecting tech firms' proprietary data and source code limit oversight of external mechanisms.

National champions may be inevitable when only a few large firms can meet the needs of the state, but these risks could be mitigated if the U.S. had fewer barriers to entry in its critical technology sector. Expanding the knowledge and resource base of the market requires improving access to data and source code, which form the basis for all software-based algorithms and services. Large data sets required for AI development are sold by a small number of American social media companies at high premiums – and unlike in China, the U.S. government is required to purchase them. High data prices and other barriers to entry also prevent nonprofit researchers from contributing to the field, resulting in a loss of in-depth research, accountability, and innovations that prioritize the social good.[79]

Bureaucratic Bloat

The bureaucratic burden of ensuring compliance with national regulations disproportionately impairs smaller firms and those who keep more strictly to the law over larger firms and those that do the bare minimum to meet standards. Nationally mandated qualification, test, and evaluation (QT&E) regulations tend to be supported – and are sometimes drafted – by America's leading technology firms, which can absorb regulatory costs more easily than their smaller competitors. In addition to reducing market competition, regulatory capture in the technology industry grants large firms an undue perception of commitment to ethical behavior, leading to additional advantages in federal procurement, contracting, and loan conditions. Once technology giants become government partners, the costs of regulatory compliance is passed to the taxpayer.

To promote competition, the United States and Europe often maintain exemptions for QT&E requirements for firms below a specific size or level of economic output. For example, the European Union initially mandated that only international firms with over 1,000 employees needed to report potential social and environmental risks to the government each year.[80] In 2024, however, these requirements were extended to upstream and downstream suppliers and subsidiaries as well as to U.S. firms with large EU customer bases even if they did not have European partners.[81] According to the European Chamber of Commerce, "It is not clear how companies will be able to comply with such requirements, as independent, third-party audits that are required to certify that they are not using

forced labor anywhere along their supply chains are difficult, and in some cases impossible, under current conditions in China."[82]

While sector-specific policies have fewer negative downstream effects, broad or overly rigid regulations drive bureaucratic bloat. The United States, like China, maintains significant breadth and agency when justifying new industrial policies as relating to the national interest or national security. Unlike Beijing, however, Washington is accountable to annual financial audits and bipartisan oversight mechanisms, making U.S. policies and initiatives far more costly to introduce and maintain than their PRC equivalents. Recent expansion of the scope of oversight of CFIUS and BIS strain these already-struggling capacities,[83] transforming what were intended to be agile and responsive entities into overlapping, multistakeholder conglomerates.

Escalatory Spirals

In the context of U.S.-China relations, American tariffs and other trade controls are implemented to motivate international policy change toward the U.S. and improve supply chain diversification and resilience. Unlike America's partners and allies, however, the Chinese state does not generally rescind or mitigate its trade restrictions in response to U.S. trade controls. Escalatory spirals such as the 2018 U.S.-China trade war and China's ongoing export cuts of critical minerals and electronics exemplify Beijing's inclination to retaliate rather than capitulate when faced with unilateral penalties from Washington.[84, 85]

Washington has further inflamed tensions by diplomatically positioning China as a military adversary rather than an economic competitor.[86] Industrial and trade policies are typically justified by threats to national security, either due to requirements in legal authorities or to secure bipartisan or public support. As these policies expand in scope and size, so do their national security justifications. Gradual rises in Washington's perceived threat level from China, bolstered by increasingly reactionary political messaging on both sides, could create a self-fulfilling prophecy where policies introduced to deter Chinese aggression counterintuitively escalate it. Near-misses and maritime incidents in the Taiwan Strait provide important reminders of how rising tensions in the highest political offices can trigger conflict breakouts at the lowest levels.[87]

Absent such a flashpoint, U.S.-China trade restrictions on commercial products and services strengthen China's authoritarian relationships and sacrifice valuable leverage that could be used to prevent future conflict. In the long run, U.S.-China decoupling strengthens China-Russia and China-North Korea cooperation in ways that may pose more risks to the international system than rewards to the United States and its allies. Decoupling also grants more power and agency to third states and multinationals, which impose two-way fees in exchange for helping importers and exporters reach new markets. For example, China is the world's largest liquefied natural gas (LNG) importer, and the United States is the most prolific LNG exporter. Due to export controls and tariffs, however, 72 percent of U.S. LNG exports are now sold at disadvantageous prices to multinational oil and gas giants like TotalEnergies and Unipec, which then resell these volumes to China.[88, 89]

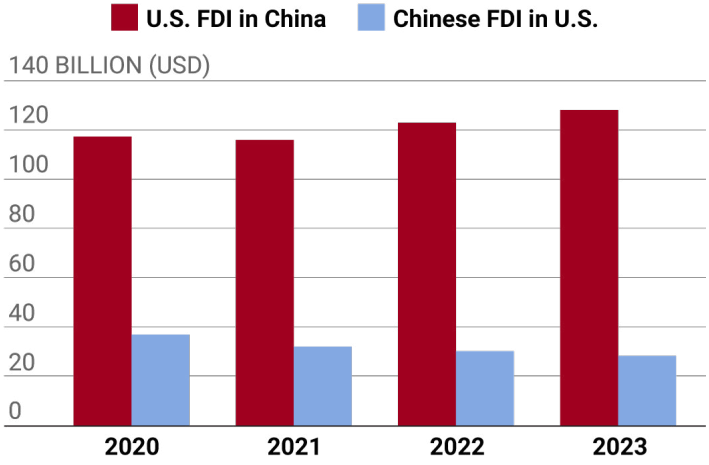
While some controls are needed to protect the most advanced defense tech from reaching Beijing, policymakers must keep in mind that the ideal U.S.-China relationship is built on international cooperation and trust, not isolationism and conflict. Trade and diplomatic cooperation prevent conflict and provide levers for de-escalation while improving economic diversity and returns.[90] Political off-ramps must be developed that enable new partnerships in nonstrategic sectors, even as restrictions are imposed on dual-use technologies. One proposal is a "clean tech détente," which would reset tariff and export controls on emerging technologies in the renewable energy sector.[91] Agriculture and beverage manufacturing are other sectors in which cooperation is unlikely to jeopardize U.S. national security or facilitate Chinese military intelligentization.

Recommendations

1. Diversify Critical Technology Investments

Regardless of strategy, the single most important metric of success of new innovation policies will be their resulting impact on investment into the American

Foreign Direct Investment



Source: U.S. Bureau of Economic Analysis

technology sector. To maintain U.S. dominance in critical technologies, Washington must invest in a broad range of competing entities, even if that means firms receive less as they grow and even if this strategy results in lower short-term returns than equivalent investments in technology giants. Leading economic experts suggest that U.S. policymakers should take a portfolio approach to investing in innovation, making small bets on a wide range of opportunities rather than continuing to prioritize national champions.[92]

In addition to supply-side policies like grants and tax incentives targeting non-R&D activities and firms outside the top six performers,[93] Washington maintains a broad suite of indirect mechanisms that can motivate domestic investment without infringing on its commitments to free and fair trade. Demand-side commitments expand market awareness of private-sector investment in emerging technologies.[94] As these subsidies can favor national champions, requirements such as friend-shoring downstream supply chains and due diligence requirements should be imposed on only the largest firms.[95]

While the U.S. government was neither structured nor intended to redirect large tax revenues into industrial policies, it is far more capable than China of accepting significant volumes of foreign investment.[96] Foreign direct investment (FDI) in the U.S. increased by $227 billion, to $5.39 trillion, in 2023, predominantly from Canada and Europe.[97] Unfortunately, recently introduced tariffs and investment restrictions threaten to reverse this trend. American outgoing direct investments exceeded incoming investments by $1.3 trillion in 2023, and with expected 25% tariffs on all Canadian imports starting in 2025,[98] the U.S. stands to lose tens of billions of dollars in FDI.

Meanwhile, cumulative foreign investment in China rose to $2.7 trillion in 2023, with significant inflows from Japan, South Korea, and Singapore.[99] In 2024, the U.S. directly invested $126.9 million in the PRC, whereas China invested only $28 million in U.S. industries.[100] Regardless of whether the Trump administration rescinds the United States-Mexico-Canada Agreement and applies these tariffs, convincing U.S. partners to redirect investments from China to North America and Europe is critical to stem China's development and diffusion of dual-use products and services.[101]

2. Promote U.S. Innovation Diffusion

Innovation diffusion is the process by which new technologies are spread internationally and applied to new sectors. To avoid the need for permanent public subsidies and maximize the impact of high-capital investments, the federal government is tasked with fostering commercial demand for cutting-edge technologies at home and abroad.[102] Public-private partnerships, international consultancies, and think tanks break down silos between innovators, investors, and regulators, accelerating the adoption and spread of new technologies.[103] Political risk advisory firms and media outlets sell the value of American products and services by bringing international awareness to the predatory market environment in China, although their transparency often makes them a target for wrongful investigations and forced closures by the Chinese Communist Party.[104]

Free trade is the second-largest contributor to innovation dynamism behind technology-sector investment. Reducing trade disparities promotes innovation diffusion, but the United States should not expect to see drastic changes in its trade deficit with China as a result of new tariffs or export subsidies. While the U.S.-China trade deficit decreased from $382 billion in 2022 to $279 billion in 2023,[105] evidence suggests this was the result of weakening domestic demand in China and discrepancies between globally

recorded figures rather than Chinese or U.S. trade barriers.[106, 107] In exchange for these limited effects, tariffs in the first Trump administration raised costs for domestic producers and importers and diminished U.S. economic well-being by 3%.[108] The same is true in China; according to the International Monetary Fund, China's approximately 5,400 subsidy policies from 2009 to 2022 had insignificant effects on subsequent export prices and quantities.[109]

Rather than impose trade barriers, the United States should design new trade and foreign infrastructure programs to provide developing nations a democratic alternative to China's Digital Silk Road initiatives. Foreign trade partnerships are highly effective in promoting innovation diffusion, particularly when the U.S. is the export partner.[110] America's trade deficit with all countries excluding China increased from $334 billion to $655 billion from 2018 to 2024,[111] demonstrating that the United States is the import partner in most new trade relationships. This trend is particularly salient in the strategically situated Indo-Pacific; while China has increased its export share to Southeast Asia by 5% since 2018, the U.S. export share climbed only 2.5% in that same period.[112]

A federal export strategy targeting key geostrategic regions would be the most efficient way to increase U.S. influence and reverse local shifts towards Beijing's political orbit. If critical technologies are deemed too sensitive or expensive to export to emerging markets, non-sensitive exports such as agricultural products can provide interim benefits and strengthen relationships while more complex investment and infrastructure programs are designed.[113]

3. Streamline and Reduce Barriers in U.S. Trade Policy

China's single-party system enables it to introduce broad, commercially unsustainable industrial policies for geostrategic purposes – specifically revenue maximization and market dominance.[114] By structuring the government to efficiently pursue these objectives, Beijing has driven down prices for some activities to an unsustainable level and introduced key bottlenecks in technology supply chains. However, as evidenced by the insignificant profit gains and lack of innovation dynamism of China's most subsidized firms, tariffs and subsidies alone fail to recoup public investment costs or drive the formation of a self-sustaining innovation ecosystem.

Rather than follow China's lead, Western countries must carve an opposing path. Thus far, Washington has responded to Chinese industrial policies by imposing trade controls, namely Section 301 and Section 232 tariffs,[115] to reduce U.S. and allied trade with China. However, these regulations tend to be incoherent, duplicative, and ineffective, and the loopholes that enable firms to obey them are rarely preferable to the status quo.[116]

End-user restrictions on military and some dual-use technologies continue to be necessary to prevent American innovations from being weaponized by foreign cyber adversaries. However, as long as U.S. enforcement mechanisms remain heterogeneous, overlapping, and fragmented, policymakers must be conservative with new trade restrictions and limit oversight mechanisms to clearly defined targets and objectives. Industry policies targeting environmental, social, and foreign governance objectives should be limited, nondiscriminatory, and temporary.

4. Promote Public-Sector Expertise and Digital Infrastructure

Public-sector technology expertise improves price formation and accountability in public programs, disincentivizing value-extractive and exploitative behavior by government contractors.[117] In addition to providing a counterweight to private-sector capital and knowledge monopolies, in-house critical technology programs are frequently better suited to public-sector needs.[118] The National Center of Artificial Intelligence has posited that military and intelligence agency talent deficits are "the greatest impediment to being AI-ready by 2025" and "the greatest inhibitor to buying, building, and fielding AI-enabled technologies."[119] For this reason, policymakers should insource private-sector talent, capacity, and expertise through programs like DARPA and ARPA-E/H/I, strengthen collaborations with nonprofit research laboratories, and publish open-source data sets where possible.

Reducing market entry costs and promoting experimentation in the private and nonprofit sectors

can improve market competition and service provision.[120] In combination with transparent, transferable public-private partnerships, these policies can also strengthen public-sector expertise. Some progress on expanding access to large data sets and cloud computing has come through public initiatives such as the National AI Research Resource Task Force and the Open Technology Fund, but more must be done to broaden the knowledge base of the field and promote free trade in ideas. A program like Germany's Sovereign Tech Agency, which uses public funds to support open-source digital infrastructure that can be used by a wide range of actors, could help democratize artificial intelligence development as well as improving cross-sector adoption of new innovations.[121]

5. Impose Costs Multilaterally, Not Unilaterally

The Trump administration has pledged to increase tariffs to upward of 60% on Chinese imports,[122] an action that threatens to push China further from the international free market system and toward retaliation and potentially rogue state status. Rather than engage in an escalation spiral with Beijing, U.S. policymakers should lean on third-party arbiters and multinational coalitions to impose costs and consequences. Reinvigorating multilateral mechanisms like the IMF, Organization for Economic Cooperation and Development, World Bank, and WTO could save hundreds of millions of dollars in implementation and oversight capacity compared to equivalent unilateral mechanisms. China has demonstrated a surprising pattern of respect for and compliance with WTO rulings,[123] as well as multilateral export control regimes more broadly. These mechanisms allow Beijing to save face domestically and demonstrate alignment with the rules-based order internationally, granting reciprocal benefits for American and Chinese policymakers and firms.

Notable critiques of international trade mechanisms are that they are slow, inefficient, and unable to benefit from privileged U.S. intelligence like their domestic regulatory equivalents. However, partner-selective mechanisms like the EU-U.S. Trade and Technology Council can coordinate regional trade and investment strategies and share the bureaucratic burden of industrial policy enforcement without unnecessarily magnifying intelligence vulnerabilities. While some multilateral agreements should be broad to impose comprehensive punitive effects, Five Eyes and other selected partners should receive additional direct intelligence on U.S. EAR rulings and be requested to adopt similar measures to magnify the effects of tariffs and sanctions. This strategy was illustrated after Biden and then-U.K. Prime Minister Rishi Sunak signed the Atlantic Declaration in 2023. Recognizing that sanctions cooperation would be difficult under current organizational structures, the United Kingdom disbanded and reformed its export control mechanisms to align more consistently with those of the United States.[124]

A required precursor of the success of large multilateral agreements is to avoid duplicating policies and practices that the U.S. condemns of China. Market competition is beneficial internationally as well as domestically, and actions taken to grant U.S. firms a significant undue advantage over their international equivalents will slow innovation, degrade trust, and increase complacency and costs. The United States was the leading recipient of WTO complaints between 2004 and 2018, and it has de facto suspended the appeals process by preventing the appointment of Appellate Body panelists.[125] Rather than continuing to deprioritize international dispute resolution mechanisms, the United States should hold China accountable to its duties and promises under the WTO and leverage its cooperation in restoring the Appellate Body to sign new multilateral agreements.[126]

Conclusion

Both China and the U.S. aggressively pursue cutting-edge technologies to enhance their domestic security and expand their foreign influence. However, China is gaining an asymmetric advantage over American firms by combining exploitation of U.S.-supported market and innovation ecosystems with large-scale industrial espionage, cyber intrusions, and protectionist policies. Rather than holding China accountable for these activities, the U.S. and Europe have chosen to introduce expansive tariff and industrial policy regimes of their own, catalyzing an international shift toward isolationism and protectionism that threatens innovation globally.

Without the same structural mechanisms that enable Chinese firms to benefit simultaneously from liberalism and authoritarianism, attempts to replicate China's "economic miracle" through trade restrictions on commercial and dual-use goods are unlikely to succeed in the United States. The scientific consensus is clear: Industrial policies in all countries should be narrow and targeted, with clear objectives and finite durations.[127] Rather than replicate the mechanisms and ecosystems developed by autocratic countries – which were only successful due to the availability of more open and technologically advanced innovation landscapes to exploit – the U.S. must reassert its commitment to the international collaborations and limited industrial policies that drove it to global technological dominance in the first place.

Encouragingly, U.S. policies to incentivize domestic innovation and democratize the critical technology landscape are showing signs of progress. In 2023, a record 5.4 million new-business applications were recorded by the Census Bureau, with high tech sectors such as information and business services seeing particularly elevated market entry and growth.[128] Despite industry assertions that Western governments will lose their strategic advantage in critical technologies due to self-limiting "ethical frameworks," these frameworks – in conjunction with nationally sponsored technology investment initiatives – are ensuring that the public good criterion is met and that as many participants as possible are able to contribute to that public good.[129]

However, balancing U.S. strategic objectives with market dynamics remains a challenge. Overreaching restrictions risk distorting domestic markets, consolidating competition, and discouraging foreign investment. Furthermore, an asymmetric preference toward domestic firms disincentivizes foreign investment and invites retaliation from U.S. competitors and adversaries, particularly China, in ways that do not benefit the U.S. or its partners.

Ultimately, the U.S. must resist the allure of emulating centralized industrial models and instead reassert its commitment to international collaboration, limited industrial policy, and the entrepreneurial spirit that has historically fueled its global leadership. After all, the true innovation that defines national progress rarely emerges from government decree alone – whether in laboratories or rented garages, it thrives in ecosystems where opportunity, collaboration, and creativity converge.

Courtney Manning is the Director of AI Imperative 2030 at The American Security Project, where she leads a team of cross-disciplinary stakeholders investigating the critical geostrategic forces driving the global AI race in the 21st century. Formerly, Manning led ASP's research portfolios on military recruitment and readiness, strategic competition with China, and emerging technology risks. Before ASP, she worked as a geopolitical risk consultant on international human rights law, political risk, and climate security in New York, where she worked with the Peruvian government to produce a new policy framework for lithium mining and the Permanent Mission of Afghanistan to rebuild the advising team, write speeches and security strategies, and coordinate sessions at the UNSC, UNGA, and Organization of Islamic Cooperation.

Endnotes

1 Reinert, J. T. (2013). In-Q-Tel: The Central Intelligence Agency as Venture Capitalist. Northwestern Journal of International Law & Business, 33(3), 677-709. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1739&context=njilb; Clifford, M. (2020, March 16). Dominic Cummings got his British Darpa. Can he make it work?. WIRED. https://www.wired.com/story/dominic-cummings-british-darpa/

2 World Bank Group. (n.d.). Global Value Chains. https://www.worldbank.org/en/topic/global-value-chains; Boyd Biomedical. (2022, August 30). The Decline of American Manufacturing and Why Today's Leaders Should Care. https://boydbiomedical.com/articles/the-decline-of-american-manufacturing

3 Hyam, B. (2023, November 29). Most Profitable Companies: U.S. vs. Rest of the World, 2023. Grow & Convert. https://www.growandconvert.com/research/most-profitable-fortune-500-companies-in-2023/

4 Long, T. (2024, November 15). Falling Behind: US Businesses Are Overlooking Emerging Tech That Could Drive Productivity. Information Technology & Innovation Foundation. https://itif.org/publications/2024/11/15/falling-behind-us-businesses-overlooking-emerging-tech-could-drive-productivity/; Durand, C. (2024, September 4). The Rise of Big Tech Is Generating Economic Stagnation. Jacobin. https://jacobin.com/2024/09/big-tech-economic-stagnation-exploitation; O'Brien, C. (2023, June 22). Like the Broader Economy, the High Tech Sector is Becoming Less Dynamic. Economic Innovation Group. https://eig.org/high-tech-dynamism/

5 Stanford Center on China's Economy and Institutions. (2024, December 1). Government Venture Capital and AI Development in China. https://sccei.fsi.stanford.edu/china-briefs/government-venture-capital-and-ai-development-china

6 Kurlantzick, J., & West, J. (n.d.). Assessing China's Digital Silk Road Initiative. Council on Foreign Relations. https://www.cfr.org/china-digital-silk-road/

7 Lew: China Cannot Lead in Innovation by Mandating Indigenous Technology. (2015, March 31). Asia Society. https://asiasociety.org/video/lew-china-cannot-lead-innovation-mandating-indigenous-technology?page=414. Brown, K. (2014, August 19). Why China Can't Innovate. The Diplomat. https://thediplomat.com/2014/08/why-china-cant-innovate/

8 China Widens Lead Over US in AI Patents After Beijing Tech Drive. (2023, October 23). Bloomberg. https://www.bloomberg.com/news/articles/2023-10-24/china-widens-lead-over-us-in-ai-patents-after-beijing-tech-drive

9 Snyder, A. (2024, May 3). Exclusive: Inside the AI research boom. Axios. https://www.axios.com/2024/05/03/ai-race-china-us-research

10 Riotta, C. (2024, December 2). China Is Outpacing US in Critical Tech Research Investments. Bank Info Security. https://www.bankinfosecurity.com/china-beating-us-in-critical-technology-research-investments-a-26952

11 Foroohar, R. (2023, February 20). The rise of kitchen table economics. Financial Times. https://www.ft.com/content/e53e4b14-4653-4b6e-a72f-d50f75e97cb7

12 Silver, L., Huang, C., Clancy, L., & Fagan, M. (2023, April 12). American Are Critical of China's Global Role – as Well as Its Relationship With Russia. Pew Research Center. https://www.pewresearch.org/global/2023/04/12/americans-are-critical-of-chinas-global-role-as-well-as-its-relationship-with-russia/

13 Beauchamp-Mustafaga, N. (2023, June 1). Chinese Next-Generation Psychological Warfare. RAND. https://www.rand.org/pubs/research_reports/RRA853-1.html

14 Leung, J. W., Robin, S., & Cave, D. (2024, August 28). ASPI's two-decade Critical Technology Tracker. Australian Strategic Policy Institute. https://www.aspi.org.au/report/aspis-two-decade-critical-technology-tracker

15 Eggers, W. D., O'Leary, J., & Pollari, K. (2023, March 16). Executing on the $2 trillion investment to boost American competitiveness. Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/public-sector/infrastructure-bill-projects-agency-execution.html

16 Tax Policy Center. (2024). How do US corporate income tax rates and revenues compare with other countries'?. https://taxpolicycenter.org/briefing-book/how-do-us-corporate-income-tax-rates-and-revenues-compare-other-countries

17 Gross domestic spending on R&D (% of GDP). (May 2023). Organisation for Economic Co-operation and Development. https://www.oecd.org/en/data/indicators/gross-domestic-spending-on-r-d.html

18 Harris, L., Benson, L. S., Gallo, M. E., Jones, A. C., Sekar, K., & Sussman, J. S. (2023). Federal Research and Development (R&D) Funding: FY2024. (Report No. R47564). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R47564

19 White House Office of Science and Technology Policy. (2022, April 5). The Biden-Haris Administration FY 2023 Budget Makes Historic Investments in Science and Technology [Press release]. https://bidenwhitehouse.archives.gov/ostp/news-updates/2022/04/05/the-biden-harris-administration-fy-2023-budget-makes-historic-investments-in-science-and-technology/. Science News. (2024, March 4). Final U.S. spending bills offer gloomy outlook for science. https://www.science.org/content/article/final-u-s-spending-bills-offer-gloomy-outlook-science

20 DiPippo, G., Mazzocco, I., & Kennedy, S. (2022). Red Ink: Estimating Chinese Industrial Policy Spending in Comparative Perspective. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220523_DiPippo_Red_Ink.pdf?VersionId=LH8ILLKWz4o.bjrwNS7csuX_C04FyEre

21 Stanford Center on China's Economy and Institutions. (2024, December 1). Government Venture Capital and AI Development in China. https://sccei.fsi.stanford.edu/china-briefs/government-venture-capital-and-ai-development-china

22 American Association for the Advancement of Science. (n.d.). Historical Trends in Federal R&D. https://www.aaas.org/programs/r-d-budget-and-policy/historical-trends-federal-rd

23 Taylor, T. (2024, October 17). A Surge in US R&D Spending. Conversable Economist. https://conversableeconomist.com/2024/10/17/a-surge-in-us-rd-spending

24 Mazzocco, I., & Featherson, R. (2024, November 19). Wins and Losses: Chinese Industrial Policy's Uneven Success. Big Data China. https://bigdatachina.csis.org/wins-and-losses-chinese-industrial-policys-uneven-success/

25 Devonshire, J. (2023, December 1). Manufacturing top targets of record-breaking cyber extortion. The Manufacturer. Albania's National Minority Differences 1 2.docx.htm

26 Birch, K., & Cochrane, D. T. (2021). Big Tech: Four Emerging Forms of Digital Rentiership. Science as Culture, 31(1), 44-58. https://www.tandfonline.com/doi/full/10.1080/09505431.2021.1932794. Saul, Derek. (2024, May 9). What Are Stock Buybacks? The Apple-Led Strategy Is Expected To Swell To $1 Trillion By 2025. Forbes. https://www.forbes.com/sites/dereksaul/2024/05/09/what-are-stock-buybacks-the-apple-led-strategy-is-expected-to-swell-to-1-trillion-by-2025/

27 McBride, J., Berman, N., Siripurapu, A. (2023, September 20). The State of U.S. Infrastructure. Council on Foreign Relations. https://www.cfr.org/backgrounder/state-us-infrastructure

28 Klein, M. U., & Hadjimichael, B. (2003). The Private Sector in Development: Entrepreneurship, Regulation, and Competitive Disciplines (p. 961). World Bank.

29 Martin, D., & Rosso, D. (2023). Chipping Away: Assessing and Addressing the Labor Market Gap Financing the U.S. Semiconductor Industry. Semiconductor Industry Association. https://www.semiconductors.org/chipping-away-assessing-and-addressing-the-labor-market-gap-facing-the-u-s-semiconductor-industry/

30 U.S. Department of Labor. (n.d.). The Good Jobs Initiative. Retrieved from Internet Archive at https://web.archive.org/web/20250116102628/https://www.dol.gov/general/good-jobs/principles.

31 Exec. Order No. 13859, 3 C.F.R. 3967-3972 (2019). https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

32 Eggers, W. D., O'Leary, J., & Pollari, K. (2023, March 16). Executing on the $2 trillion investment to boost American competitiveness. Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/public-sector/infrastructure-bill-projects-agency-execution.html

33 Artificial Intelligence for the American People. (n.d.). Trumpwhitehouse.archives.gov. https://trumpwhitehouse.archives.gov/ai/executive-order-ai/

34 Friedman, R. A., McAllister, A. K., Crusius, E. S., Zales, M. A., & Hubner, A. K. (2022, December 27). 2023 NDAA Tightens Controls on Chinese Semiconductors in Government Contractor Supply Chains. Holland & Knight. https://www.hklaw.com/en/insights/publications/2022/12/2023-ndaa-tightens-controls-on-chinese-semiconductors-in-government

35 Mazzucato, M., Schaake, M., Krier, S., & Entsminger, J. (2022). Governing artificial intelligence in the public interest. UCL Institute for Innovation and Public Purpose, Working Paper Series (IPP WP 2020-12). https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/governing-artificial-intelligence-public-interest-cpc.pdf

36 White House. (2024, March 28). FACT SHEET: Vice President Harris Announces OMB Policy to Advance Governance, Innovation, and Risk Management in Federal Agencies' Use of Artificial Intelligence [Fact sheet]. Retreieved from Internet Archive at https://web.archive.org/web/20250118023224/https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/28/fact-sheet-vice-president-harris-announces-omb-policy-to-advance-governance-innovation-and-risk-management-in-federal-agencies-use-of-artificial-intelligence/.

37 Woods, L., & Kashen, J. (2024, April 17). CHIPS Act Child Care Requirements Already Showing Promise. The Century Foundation. https://tcf.org/content/commentary/chips-act-child-care-requirements-already-showing-promise/ https://tcf.org/content/commentary/chips-act-child-care-requirements-already-showing-promise/

38 Office of the United States Trade Representative. (n.d.). Mission of the USTR. https://ustr.gov/about-us/about-ustr; Office of the Chief Council for Industry and Security. (2020). Legal Authority. https://www.bis.gov/sites/default/files/files/legal-authorities-2020-with-hyperlinks.pdf

39 Office of Foreign Assets Control. (n.d.). Mission. https://ofac.treasury.gov/

40 Office of the Chief Council for Industry and Security. (2020). Legal Authority. https://www.bis.gov/sites/default/files/files/legal-authorities-2020-with-hyperlinks.pdf

41 Office of Conventional Arms Threat Reduction. (n.d.). About Us – Office of Conventional Arms Threat Reduction. https://www.state.gov/about-us-office-of-conventional-arms-threat-reduction/; U.S. Department of State Bureau of Political-Military Affairs. (n.d.). Directorate of Defense Trade Controls. https://www.state.gov/bureaus-offices/under-secretary-for-arms-control-and-international-security-affairs/bureau-of-political-military-affairs/directorate-of-defense-trade-controls-pm-ddtc/

42 U.S. Department of State Bureau of Political-Military Affairs. (n.d.). Directorate of Defense Trade Controls. https://www.state.gov/bureaus-offices/under-secretary-for-arms-control-and-international-security-affairs/bureau-of-political-military-affairs/directorate-of-defense-trade-controls-pm-ddtc/

43 Congressional Research Service. (2025, January 31). U.S. Tariff Policy: Overview (Report No. IF11030). https://crsreports.congress.gov/product/pdf/IF/IF11030

44 Congressional Research Service. (2025, January 31). U.S. Tariff Policy: Overview (Report No. IF11030). https://crsreports.congress.gov/product/pdf/IF/IF11030

45 U.S. Mission China. (2024, May 24). Four-Year Review of Actions Taken in the Section 301 Investigation: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation. https://china.usembassy-china.org.cn/four-year-review-of-actions-taken-in-the-section-301-investigation/

46 Cheng, S. (2024, November 27). Breaking down the world's tariffs against China's tech industry. Rest of World. https://restofworld.org/2024/china-tech-tariffs-which-countries-will-impose/

47 Jackson, J. K. (2020). The Committee on Foreign Investment in the United States (CFIUS) (Report No. RL33388). Congressional Research Service. https://crsreports.congress.gov/product/pdf/RL/RL33388

48 Congressional Research Service. (2024, December 9). Committee on Foreign Investment in the United States (CFIUS) (Report No. IF10177). https://crsreports.congress.gov/product/pdf/IF/IF10177

49 Congressional Research Service. (2024, December 10). Regulation of U.S. Outbound Investment to China (Report No. IF12629). https://crsreports.congress.gov/product/pdf/IF/IF12629

50 U.S. Department of the Treasury. (n.d.). Outbound Investment Security Program. https://home.treasury.gov/policy-issues/international/outbound-investment-program

51 Bureau of Industry & Security. (2023, November 17). General Prohibitions. https://www.bis.doc.gov/index.php/documents/regulation-docs/413-part-736-general-prohibitions/file

52 Bureau of Industry & Security. (n.d.). Promoting Human Rights and Democracy. https://www.bis.doc.gov/index.php/human-rights

53 U.S. Department of State. (2022, June 21). Implementation of the Uyghur Forced Labor Prevention Act [Press release]. Retrieved from Internet Archive, at https://web.archive.org/web/20250106034552/https://www.state.gov/implementation-of-the-uyghur-forced-labor-prevention-act/

54 Congressional Research Service. (2024, November 7). Human Rights and Anti-Corruption Sanctions: The Global Magnitsky Human Rights Accountability Act (Report No. IF10576). https://crsreports.congress.gov/product/pdf/IF/IF10576

55 U.S. Department of State. (n.d.). Export Controls Policy. Retrieved from Internet Archive, at https://web.archive.org/web/20250123172742/https://www.

state.gov/nonproliferation-export-controls/.

56 World Trade Organization. (n.d.). WTO in Brief. https://www.wto.org/english/thewto_e/whatis_e/inbrief_e/inbr_e.htm

57 United Nations Trade & Development. (n.d.). Tariff trends mostly downward, but non-tariff measures increasingly used. https://sdgpulse.unctad.org/trade-barriers/; Kimberly Process. (n.d.). Home. https://www.kimberleyprocess.com/

58 U.S. Department of State. (n.d.). Multilateral Trade Affairs. https://www.state.gov/multilateral-trade-affairs/

59 Hirschman, A. O. (1958). The Strategy of Economic Development. Yale University Press; Holz, C. A. (2011). The unbalanced growth hypothesis and the role of the state: The case of China's state-owned enterprises. Journal of Development Economics, 96(2), 220-238. https://www.sciencedirect.com/science/article/abs/pii/S0304387810001264

60 Toole, A. A., Miller, R. D., & Rada, N. (2020). Intellectual Property and the U.S. economy: Third edition. U.S. Patent and Trademark Office. https://www.uspto.gov/sites/default/files/documents/uspto-ip-us-economy-third-edition.pdf

61 Lawrence, R. Z., & Litan, R. E. (1987, May). Why Protectionism Doesn't Pay. Harvard Business Review. https://hbr.org/1987/05/why-protectionism-doesnt-pay

62 Autor, D., Beck, A., Dorn, D., & Hanson, G. (2024). Help for the Heartland? The Employment and Electoral Effects of the Trump Tariffs in the United States. NBER Working Paper Series. https://economics.mit.edu/sites/default/files/2024-08/Help_for_the_Heartland_20240815.pdf

63 Kamal, F., McCloskey, J., & Ouyang, W. (2023, February 16). Domestic and foreign-owned multinationals in the US economy: Insights from newly linked data. Centre for Economic Policy Research. https://cepr.org/voxeu/columns/domestic-and-foreign-owned-multinationals-us-economy-insights-newly-linked-data

64 Congressional Research Service. (2025, January 31). U.S. Tariff Policy: Overview (Report No. IF11030). https://crsreports.congress.gov/product/pdf/IF/IF11030. York, Erika. (2024, November 6). Revenue Estimates of Trump's Universal Baseline Tariffs. Tax Foundation. https://taxfoundation.org/blog/trump-tariffs-revenue-estimates/

65 Weisman, D. L., & Pfeinfenberger, J. P. (2003). Efficiency as a Discovery Process: Why Enhanced Incentives Outperform Regulatory Mandates. The Electricity Journal, 16(1), 55-62. https://www.sciencedirect.com/science/article/abs/pii/S1040619002004153

66 Semiconductor Industry Association. (2025, January 22). CHIPS Incentives Awards. https://www.semiconductors.org/chips-incentives-awards

67 White, J. (2023, November 21). Ford scales back Michigan battery plant, restarts construction. Reuters. https://www.reuters.com/business/autos-transportation/ford-scales-back-michigan-battery-plant-restarts-construction-2023-11-21/

68 Agarwal, R. (2023, September). Industrial Policy and the Growth Strategy Trilemma. International Monetary Fund. https://www.imf.org/en/Publications/fandd/issues/Series/Analytical-Series/industrial-policy-and-the-growth-strategy-trilemma-ruchir-agarwal

69 Aviation Week Network. (2017, May 5). COMAC launches C919 inaugural flight. http://atwonline.com/airframes/comac-launches-c919-inaugural-flight

70 India woos Tesla by slashing import duty on EVs to 15% from 70-100%. (2024, March 16). The Hindu. https://www.thehindu.com/news/national/india-woos-tesla-by-slashing-import-duty-on-evs-to-15-from-70-100/article67955547.ece

71 Daga, A. (2024, January 26). Indonesia's nickel policy looks fragile. Reuters. https://www.reuters.com/breakingviews/indonesias-nickel-policy-looks-fragile-2024-01-26/

72 AmCham China. (2023, March 5). 2023 China Business Climate Survey Report. https://www.amchamchina.org/2023-china-business-climate-survey-report/

73 Fan, X. (2024, May 10). European Chamber Calls for Action to Restore Business Confidence. The European Union Chamber of Commerce in China. https://www.europeanchamber.com.cn/en/publications-business-confidence-survey

74 Allen, G. C., Benson, E., & Reinsch, W. A. (2022). Improved Export Controls Enforcement Technology Needed for U.S. National Security. Center for Strategic & International Security. https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security; Coalition for a Prosperous America. (2021, July 22). CPA: SEC Must Implement Holding Foreign Companies Accountable Act Without Delay. https://prosperousamerica.org/cpa-sec-must-implement-holding-foreign-companies-accountable-act-without-delay/

75 Dudley, R. (2023, July 19). "At What Point Does Profit Trump Safety?" Ex-National Cyber Director Presses Software Regulation Amid High-Profile Hacks. ProPublica. https://www.propublica.org/article/cybersecurity-expert-software-regulation-amid-hacks

76 Biden, J. (2024). National Cybersecurity Strategy Implementation Plan. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/NCSIP-Version-2-FINAL-May-2024.pdf

77 Manning, C. (2024, June 5). Shaming Microsoft won't strengthen US cybersecurity. It's time for alternatives. The Hill. https://thehill.com/opinion/technology/4705671-shaming-microsoft-wont-strengthen-us-cybersecurity-its-time-for-alternatives/

78 Cybersecurity & Infrastructure Security Agency. (n.d.). Federal Zero Trust Strategy. https://zerotrust.cyber.gov/federal-zero-trust-strategy/

79 Mazzucato, M., Schaake, M., Krier, S., & Entsminger, J. (2022). Governing artificial intelligence in the public interest. UCL Institute for Innovation and Public Purpose, Working Paper Series (IPP WP 2020-12). https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/governing-artificial-intelligence-public-interest-cpc.pdf

80 European Commission. (n.d.). Corporate sustainability reporting. https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en

81 Lakhdhir, D. (2024, July 15). The EU Due Diligence Directive: Implications for U.S. Companies. American Bar Association. https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-july/eu-due-diligence-directive-implications-us-companies/

82 Fan, X. (2024, May 10). European Chamber Calls for Action to Restore Business Confidence. The European Union Chamber of Commerce in China. https://www.europeanchamber.com.cn/en/publications-business-confidence-survey

83 Shenai, N., Hurewitz, B. J., Meltzer, R. I., & Maurer, A. (2024, December 6). BIS Issues Sweeping Additional Resources on Semiconductors and Advanced Computing, Entity List Designations. WilmerHale. https://www.wilmerhale.com/en/insights/client-alerts/20241206-bis-issues-sweeping-additional-restrictions-on-semiconductors-and-advanced-computing-entity-list-designations

84 Jian, Y. (2024, December 1). China sharpens trade war tools ahead of Trump's arrival. Asia Times. https://asiatimes.com/2024/12/china-sharpens-trade-war-tools-ahead-of-trumps-arrival/

85 U.S. Mission China. (2024, May 24). Four-Year Review of Actions Taken in the Section 301 Investigation: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation. https://china.usembassy-china.org.cn/four-year-review-of-actions-taken-in-the-section-301-investigation/

86 O'Hanlon, M. E. (2023, June). Getting China right: Resoluteness without overreaction. Brookings. https://www.brookings.edu/articles/getting-china-right-resoluteness-without-overreaction/

87 Taiwan Strait: footage released of near miss between Chinese warship and US destroyer. (2023, June 3). The Guardian. https://www.theguardian.com/world/2023/jun/05/taiwan-strait-footage-released-of-near-miss-between-chinese-warship-and-us-destroyer

88 Schmidt, J., Samuel, A., & Shukla, S. (2024, January 24). Liquified Natural Gas Has Limited Impact in Displacing Coal Emissions. National Resources Defense Council. https://www.nrdc.org/bio/jake-schmidt/us-liquified-natural-gas-has-limited-impact-coal

89 Manning, C. (2024, October 16). Perspective – The U.S.-China LNG Export Dilemma: Reclaiming Leverage in an Imbalanced Trade Relationship. American Security Project. https://www.americansecurityproject.org/us-china-lng-competition/

90 Martin, B. (2024, February 23). Interdependence and Its Discontents: Why Would Nations with Incentives to Avoid It Go to War? RAND. https://www.rand.org/pubs/commentary/2024/02/interdependence-and-its-discontents-why-would-nations.html

91 Busby, J., Goldman, J., Villalobos, F. E. (2024, November 19). Can the U.S. and China Ease Tensions with a Clean Tech Détente?. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/11/can-the-us-and-china-ease-tensions-with-a-clean-tech-detente?lang=en

92 Jones, B. F. (2021). Science and Innovation: The Under-Fueled Engine of Prosperity. Aspen Economic Strategy Group. https://www.economicstrategygroup.org/wp-content/uploads/2021/11/8-Jones.pdf; Wilson, C., Grubler, A., Bento, N., Healy, S., De Stercke, S., & Zimm, C. (2020). Granular technologies to accelerate decarbonization. Science, 386(6486), 36-39. https://www.science.org/doi/10.1126/science.aaz8060

93 CBInsights. (2023, December 6). The future of big tech in 10 charts. https://www.cbinsights.com/research/report/big-tech-future-charts/

94 Cunningham, P. (2009). Demand-side Innovation Policies. Pro Inno Europe. https://wbc-rti.info/object/document/7210/attach/TrendChart_demand-side_policies_innovation_needs.pdf

95 Lee, J., Jun, S., & Lee, C. (2022). Does demand-side innovation drive lock-in? Global evidence from solar energy in 155 countries. Energy Research & Social Science, 89(1). https://www.sciencedirect.com/science/article/pii/S2214629622000469

96 Asdurian, A., Derrick, A., & McMahon, A. (2024). Foreign Direct Investment in the United States. Department of Commerce, Office of the Under Secretary for Economic Affairs. https://www.commerce.gov/sites/default/files/2024-10/FDI-Report-Final.pdf

97 Bureau of Economic Analysis. (2024, July 23). Direct Investment by Country and Industry. https://www.bea.gov/data/intl-trade-investment/direct-investment-country-and-industry

98 Pitas, C. (2024, November 26). Trump vows new Canada, Mexico, China tariffs that threaten global trade. Reuters. https://www.reuters.com/world/us/trump-promises-25-tariff-products-mexico-canada-2024-11-25/

99 Interesse, G. (2024, November 6). China's FDI Trends 2024: Key Sources, Destinations, and Sectors. China Briefing. https://www.china-briefing.com/news/chinas-fdi-trends-2024-key-sources-destinations-and-sectors/

100 Bureau of Economic Analysis. (2024, July 23). Direct Investment by Country and Industry, 2023 [News release]. https://www.bea.gov/sites/default/files/2024-07/dici0724.pdf

101 Interesse, G. (2024, November 6). China's FDI Trends 2024: Key Sources, Destinations, and Sectors. China Briefing. https://www.china-briefing.com/news/chinas-fdi-trends-2024-key-sources-destinations-and-sectors/

102 Paschkewitz, J., & Patt, D. (Fall 2023). No, We Don't Need Another ARPA. Issues in Science and Technology, 40(1), 93-97. https://issues.org/arpa-catalyze-diffusion-paschkewitz-patt/

103 Bateman, J. (2022). U.S.-China Technological "Decoupling". Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_US-China_Decoupling_final.pdf

104 Butts, D. (2023, May 18). US-based Forrester Research to close China office amid Beijing's crackdown on foreign adversaries. South China Morning Post. https://www.scmp.com/tech/article/3220892/us-based-forrester-research-close-china-office-amid-beijings-crackdown-foreign-advisories

105 Bureau of Economic Analysis. (2024, February 7). U.S. International Trade in Goods and Services, December and Annual 2023 [News release]. https://www.bea.gov/news/2024/us-international-trade-goods-and-services-december-and-annual-2023

106 Gourinchas, P., Pazarbasioglu, C., Srinivasan, K., & Valdes, R. (2024, September 12). Trade Balances in China and the US are Largely Driven by Domestic Marco Forces. International Montary Fund. https://www.imf.org/en/Blogs/Articles/2024/09/12/trade-balances-in-china-and-the-us-are-largely-driven-by-domestic-macro-forces

107 Clark, Hunter. (2025, February 26). U.S. Imports from China Have Fallen by Less Than U.S. Data Indicate. Federal Reserve Bank of New York. https://libertystreeteconomics.newyorkfed.org/2025/02/u-s-imports-from-china-have-fallen-by-less-than-u-s-data-indicate/

108 Stackpole, T. (2024, December 2). What the Last Trump Tariffs Did, According to Researchers. Harvard Business Review. https://hbr.org/2024/12/

what-the-last-trump-tariffs-did-according-to-researchers

109 Rotunno, L., & Ruta, M. (2024). Trade Implications of China's Subsidies. IMF Working Papers, 2024(180). https://www.elibrary.imf.org/view/journals/001/2024/180/article-A001-en.xml

110 Jiang, Y. (2014). 4 – Potential effects of foreign trade on development. In Jiang, Y (Ed.), Chandos Asian Studies Series (pp. 45–61). Chandos Publishing. https://www.sciencedirect.com/science/article/abs/pii/B9781843347620500049; Hakura, D., & Jaumotte, F. (2001). Chapter 5: The Role of Trade in Technology Diffusion. In Fosu, A. K., Nsouli, A. M., & Varoudakis, A. (Eds.), Policies to Promote Competitiveness in Manufacturing in Sub-Saharan Africa. International Monetary Fund. https://www.elibrary.imf.org/display/book/9789264187054/ch005.xml; Geng, D., & Kali, R. (2021). Trade and innovation: Unraveling a complex nexus. International Journal of Innovation Studies, 5(1), 23-34.https://www.sciencedirect.com/science/article/pii/S2096248721000011

111 Soltani, Ehsan. (2025, January 7.) U.S. Trade Deficit Shifts: 28% Decline with China but 96% Surge with Rest of World. Voronoi. https://www.voronoiapp.com/trade/-US-Trade-Deficit-Shifts-28-Decline-with-China-but-96-Surge-with-Rest-of-World-3591

112 Pitas, C. (2024, November 26). Trump vows new Canada, Mexico, China tariffs that threaten global trade. Reuters. https://www.reuters.com/world/us/trump-promises-25-tariff-products-mexico-canada-2024-11-25/

113 Sabala, E. & Gale, F. (2024, August 6). U.S. Agricultural Exports in Southeast Asia. USDA Economic Research Service. https://www.ers.usda.gov/publications/pub-details?pubid=109671

114 Barwick, P. J., Kalouptsidi, M., & Zahur, N. B. (2021). Industrial Policy: Empirical Evidence from China's Shipbuilding Industry (Report No. 261). CATO Institute. https://panlebarwick.github.io/papers/Yr23_ChinaShipyard.pdf

115 Bureau of Industry & Security. (n.d.). Section 232 Investigations: The Effects of Imports on the National Security. https://www.bis.doc.gov/index.php/other-areas/office-of-technology-evaluation-ote/section-232-investigations

116 Ferrari, J. G., & Rosenblatt, M. (2024). Preparing Supply Chains for a Coming War. American Enterprise Institute. https://www.aei.org/wp-content/uploads/2024/02/Preparing-Supply-Chains-for-a-Coming-War.pdf

117 Mazzucato, M. (2015). Entrepreneurial State: Debunking Public Vs. Private Sector Myths. Anthem Press.

118 Mazzucato, M., Schaake, M., Krier, S., & Entsminger, J. (2022). Governing artificial intelligence in the public interest. UCL Institute for Innovation and Public Purpose, Working Paper Series (IPP WP 2020-12). https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/governing-artificial-intelligence-public-interest-cpc.pdf

119 National Security Commission on Artificial Intelligence. (n.d.). Chapter 6: Technical Talent in Government. https://reports.nscai.gov/final-report/chapter-6

120 Paschkewitz, J., & Patt, D. (Fall 2023). No, We Don't Need Another ARPA. Issues in Science and Technology, 40(1), 93-97. https://issues.org/arpa-catalyze-diffusion-paschkewitz-patt/

121 Sovereign Tech Agency. (n.d.). Our Mission. https://www.sovereign.tech/mission/

122 Xing, Y. (2024, November 20). Trump's 60% tariffs on Chinese goods would bite Apply the hardest. Nikkei Asia. https://asia.nikkei.com/Opinion/Trump-s-60-tariffs-on-Chinese-goods-would-bite-Apple-the-hardest

123 Bacchus, J., Lester, S., & Zhu, H. (2018, November 15). Disciplining China's Trade Practices at the WTO: How WTO Complaints Can Help Make China More Market-Oriented. CATO Institute. https://www.cato.org/policy-analysis/disciplining-chinas-trade-practices-wto-how-wto-complaints-can-help-make-china-more; The Select Committee on the Strategic Competition Between the United States and The Chinese Communist Party. (2023). RESET, PREVENT, BUILD: A Strategy to Win America's Economic Competition with the Chinese Communist Party. https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/reset-prevent-build-scc-report.pdf

124 Manning, C. (2024, January 26). Trans-Atlantic Export Controls: Leaping Promises, Lagging Oversight. American Security Project. https://www.americansecurityproject.org/leaping-promises-lagging-oversight/

125 Congressional Research Service. (2024, July 17). Dispute Settlement in the WTO and U.S. Trade Agreements. (Report No. IF10645). https://crsreports.congress.gov/product/pdf/IF/IF10645

126 McDonald, B., Nielson, J., Signoret, J., & Keck, A. (2022). Subsidies, Trade, and International Cooperation. International Monetary Fund. https://www.imf.org/-/media/Files/Publications/analytical-notes/2022/English/ANEA2022001.ashx

127 Gourinchas, P., Pazarbasioglu, C., Srinivasan, K., & Valdes, R. (2024, September 12). Trade Balances in China and the US are Largely Driven by Domestic Marco Forces. International Montary Fund. https://www.imf.org/en/Blogs/Articles/2024/09/12/trade-balances-in-china-and-the-us-are-largely-driven-by-domestic-macro-forces

128 Pardue, L. (2024, April 25). In Brief: The Recent Rise in US Labor Productivity. Aspen Economic Strategy Group. https://www.economicstrategygroup.org/publication/in-brief-us-labor-productivity/

129 Kak, A. (2024). AI Nationalism(s): Global Industrial Policy Approaches to AI. AI Now. https://ainowinstitute.org/wp-content/uploads/2024/03/AI-Nationalisms-Exec-Summary.pdf

From left, Gen. Timothy Haugh, director of the National Security Agency; Kash Patel, FBI director; Tulsi Gabbard, National Intelligence director; John Ratcliffe; CIA director; and Lt. Gen. Jeffrey Kruse, Defense Intelligence Agency director, testify at the U.S. Senate Intelligence Committee hearing on "Worldwide Threats," on March 25, 2025, in Washington, D.C.. (Maansi Srivastava for the Washington Post)

Overcoming the Challenges of Incentivizing Cybersecurity

Maxime Lamothe-Brassard

The costs associated with global cybercrime have increased every year, a trend projected to continue, exceeding $15 trillion by 2029.[1] How can the government create an incentive structure that drives organizations to improve cybersecurity? While considering that question, it is important to remember that, for the most part, different organizations and their operations are idiosyncratic. The monumental challenge of finding an approach that works well for all will likely require cooperation between the public and private sectors.

One major difference separating private organizations and the public sector is the need to generate revenue through sales. Profit-driven businesses focus on maximizing efficiencies and streamlining processes, naturally leading them to seek the most inexpensive way to meet the letter of the law irrespective of its intent. This is not businesses seeking to "game the system" but rather their attempt to adapt to new rules (and often, expenses) without disrupting operations.

Regulations directing businesses to invest in additional training, technology, or processes represent new costs.[2] All things being equal, whoever finds the most efficient way to address these new expenses gains a minor advantage over their competitors. This may seem obvious, but it's important to keep in mind

anytime new legislation aimed at influencing behavior is under consideration. If a regulation can be satisfied in inexpensive ways that fail to achieve the regulator's intentions, it will be.

Within the current structure of the cybersecurity industry, there are two major phenomena: the frequency and severity of cyberattacks continue to escalate,[3] and the few large vendors[4] that provide the lion's share of cybersecurity protections have not solved the issue. A paradigm shift may be what is necessary to reverse the trend of escalating cyberattacks and improve the security posture of both the private and public sectors.

This is not meant to disparage the current top vendors, whose work prevents the majority of breaches. It is simply an assessment of where cybersecurity is today and has been for a while. The field is locked in a reactive cycle where today's cybersecurity is mostly an amalgamation of yesterday's fixes and patches.

Business organizations respond to various incentives, but there are two that stand head and shoulders above the rest: customer demand and government regulation. Unfortunately, customer demand alone has proven insufficient to drive cybersecurity in the right direction. While well-considered regulations may lead businesses to improve their cybersecurity practices, they also run the risk of introducing unintended and negative consequences. Effective regulations will incentivize organizations to improve cybersecurity by ensuring their tenets do not hinder core business operations.

Another difficulty in writing effective cybersecurity regulations is the disparate speeds at which government and technology advance. Government action is generally assumed to be slow and methodical while technology moves at a lightning pace. Legislators require time to gather information, consult with constituents, explore solutions, and so on. Technology has few barriers to its advancement, and new innovations can quickly overturn years of established processes.

Since it is unrealistic to ask legislators to stay on top of technological advancements and adapt regulations in real time, focusing on basic security principles makes sense. Regulators should consider taking a "build up from the floor" approach. Start with a minimal foundation of widely applicable rules, then monitor their impact before crafting further solutions. This way, progress can be made while minimizing undesirable side effects.

Legislative Considerations

Cybersecurity legislation is a sensitive topic because it touches upon the two greatest risk concerns of business leaders: regulatory compliance and security. Industry studies rank both of these risks as primary business concerns, with one or the other being a top consideration depending on the source.[5, 6] This shows that organizations are as worried about running afoul of regulations as they are of being the victim of a data breach.

Legislators should remain keenly aware of this concern. If they make a misstep, the result will be organizations scrambling to achieve technical compliance rather than focusing on building stronger security practices.[7] This result is worse than doing nothing, as companies will sacrifice resources to stay out of legal trouble while remaining as vulnerable as before.

There is also the problem of the various cybersecurity needs of different industries and organizations. To draw a parallel, imagine the complications of trying to regulate the physical security of buildings. Perhaps legislators decide to start with something basic, like mandating that all exterior doors of a building must have a lock. This would seem to improve security for everything from garden sheds to the Pentagon. Yet, a criminal with a lockpick kit or a crowbar is already capable of defeating that security, so more must be done. What should happen next?

While the garden shed and the Pentagon are both buildings, they have distinctly different security needs. It may be fair to ask if the garden shed's security is worth addressing at all, given the generally relatively low value of its contents. Perhaps legislators only want to focus on securing buildings holding a certain amount of valuable goods or sensitive information. Then there are buildings such as hospitals and fire stations where rapid ingress or egress is critical to

operations. How should legislators secure those without impeding their core mission?

This analogy is not perfect, but it illustrates how security problems become increasingly complex as specific use cases are considered. In this way, it is analogous to trying to secure endpoints, networks, internet-connected devices, operational technology, and enterprises across diverse industries. At the micro level, writing cybersecurity guidelines for a specific business is achievable. Tackling the problem at a macro level by creating rules for multiple industries is exponentially more difficult.

The point of this intellectual exercise is to demonstrate the importance of scoping, or targeting, legislation to address a specific use case. Legislating cybersecurity rules for banks is a tall order, given the various types of banks and their internal and external processes. However, a viable starting point for making some progress can be found by asking, "What is something common to all banks that should absolutely be secure?" This works because the focus changes from securing "banks" to protecting a specific process all banks perform.

Overcoming Public Sector Inertia

Government agencies spend lots of time crafting policy, soliciting public feedback, considering the impacts of their rules, and so on. On the other hand, a common vulnerability and exposure, a publicly disclosed computer security flaw, is commonly exploited within minutes of being published.[8] How can a deliberate and collaborative government craft useful guidance to prevent attacks that arise immediately after vulnerabilities are disclosed?

To reiterate, the goal is to stop successful cyberattacks from occurring. This is much different than responding to successful ones. The government is well-versed in emergency response operations when dealing with natural disasters, public unrest, and similar foreseeable calamities. In these cases, public institutions have extensive, multistep disaster risk management plans for recovering from an event. Crafting incentives that proactively prevent disasters caused by people is more difficult.

In a similar vein, governments have general plans for dealing with unexpected physical attacks.

Roman Proskurovskyi, the deputy director of information security at the National Bank of Ukraine speaks about the resilience of the country's banking system to cyber intrusions on Feb. 8, 2024 in Kyiv, Ukraine. (hurricanehank / Global Images Ukraine via Getty Images)

This offers legislators a good starting place for developing ideas to address cybersecurity problems. To combat unexpected physical attacks, governments often employ:

- **Intelligence-gathering** – Collecting data on adversaries, monitoring communications, and analyzing threat patterns
- **Strategic risk assessment** – Evaluating vulnerabilities and potential targets, and allocating resources to areas at greatest risk
- **Coordinating responses** – Establishing command-and-control structures to govern and coordinate the participations of multiple allies and agencies
- **Training exercises** – Creating and performing simulated attack-and-response scenarios
- **Resource stockpiling and redundancy plans** – Devising strategies to ensure key organizations retain access to crucial resources and critical systems remain operational
- **Preventive diplomacy** – Forming bonds and alliances with others to deter aggression from hostile actors

These suggestions share some common ground with steps businesses currently take to address cyberthreats. For example, large organizations often do red-teaming and tabletop exercises simulating cyberattacks as part of maintaining their security posture. Any business large enough to have a security operations center performs information and intelligence gathering on a daily basis. Cases where public and private sector risk-reduction practices overlap can provide a good framework for discussing regulatory incentives.

Another good practice when considering regulatory schemes is to begin with the end goal in mind. What steps will ensure organizations implement better security rather than focusing on achieving technical compliance? Unintrusive measures that minimize impacts on a business' core mission, such as tax breaks, subsidies, and the provision of publicly available resources, will be met with less resistance.

While the size and shape of any tax incentives and subsidies is a discussion best left to economists, the core concept is simple: Making the adoption of strong cybersecurity practices less expensive will increase compliance. The more organizations must pay out of pocket for cybersecurity, the more likely they are to take risks in implementing it.

Open Government vs. Open Source

Providing public resources is another effective way to encourage and enable the private sector to improve cybersecurity performance. The public sector already actively assists businesses by providing frameworks like NIST CSF 2.0 and publishing the CISA Known Exploited Vulnerabilities Catalog.[9, 10] The cybersecurity field also draws upon several open-source projects to perform critical work including Sigma, VirusTotal, Metasploit, OWASP, TheHive, YETI, and others.[11, 12, 13, 14, 15, 16]

In fact, cybersecurity regularly embraces and relies upon open-source tools, platforms, and organizations. Essential cybersecurity apps such as Wireshark, NMAP, Burp Suite, SNORT, OSSEC and Aircrack-ng are just a few examples.[17] All of these projects exist to meet a security need that the public and private sector have not. Each highlights an opportunity for governments to incentivize better cybersecurity by taking a leading role. For example, if the government added its cyberthreat knowledge to VirusTotal, or created and maintained a similar service, organizations would utilize it. If the government develops and offers effective cybersecurity resources to the public, they will be adopted.

The same idea also applies to offering public cybersecurity certifications, education, and training. By alleviating some of the financial and training overhead associated with cybersecurity, public institutions can help private organizations directly improve their security practices.

Increased Transparency Helps Everyone

The popularity of open-source resources might mistakenly be attributed to their being freely available. While this is certainly one factor that drives their adoption, it is not necessarily the primary one. What truly makes open-source projects valuable to security professionals is their transparency. An analyst never has to guess how an open-source tool works. They

can simply review the documentation or examine the code themselves.

Transparency not only fosters understanding but also drives innovation. When people know how something operates, they can envision new ways to use it. One need only to look at the popular open-source kernel Linux to see real-world examples of this. The Linux kernel was released as an open-source project by Linus Torvalds in 1991.[18] Today there are approximately 1,000 different distributions of Linux operating systems, including ones catering specifically to cybersecurity professionals.[19]

The phenomenal growth of Linux, due to its transparency and open-source foundations, is something that can be broadly replicated across the security operations field. Right now, most of the private sector relies on large cybersecurity vendors whose practices are not transparent. If a threat is detected and prevented, the public may or may not hear about it. When a cyberattack succeeds, only the affected organization knows why existing protections failed. This kind of secrecy stifles innovation.

These cybersecurity vendors sell black-box solutions and later offer apologies when they fail. Without knowing the specifics of why a product failed, it is difficult to prevent future failures. While numerous threat research papers that often contain a section on indicators of compromise, which note characteristics of a cyber threat, these artifacts appear after a cyberattack succeeds. Knowing the steps that led a specific security solution to fail is as important as knowing how to identify an attack after it succeeds. Unfortunately, most security vendors cannot share such information without revealing sensitive information on how their product works.

Better visibility into all aspects of those failures would allow all cybersecurity efforts to advance more quickly. The benefits of transparency could be realized without requiring private companies to divulge trade secrets or surrender intellectual property. However, it is important to move beyond the current norm of security vendors saying, "Trust us, you're protected," then merely apologizing when things go wrong. Specific details about points of failure allow everyone in the cybersecurity space to learn from a mistake.

Foreseeing Unintended Consequences

When discussing the nature of incentives, it is often useful to reference the carrot-and-stick approach. Expanded government services, tax incentives, and public training represent the carrot approach to influencing cybersecurity. The government can also try to shape cybersecurity practices through the stick of punishment, fines, and incarceration. While the stick may be appropriate for certain egregious and reckless behaviors, it often triggers unintended consequences that detract from its effectiveness.

For example, if violating a regulation carries heavier penalties than the consequences of a potential breach, focus will be placed on legal compliance over protecting the organization. Ideally, pursuing legal compliance should lead directly to improving an organization's cybersecurity posture. Yet for every instance where this is not the case, resources spent on achieving compliance are a net loss. The business can show auditors that they've checked the correct legal boxes, but their infrastructure is as insecure as before.

To further illustrate the potential dangers of ill-considered legislation, let's look at the topic of ransomware payments. Some cybersecurity professionals have proposed that the government make paying ransom to cybercriminals illegal.[20] At first glance this approach seems to solve the problem. If criminals cannot make money from ransoming data, there would be no motivation to do so. The idea also aligns with the popular ethos of "we do not negotiate with terrorists."

Yet, outlawing the paying of those ransoms only restricts the options of businesses and public organizations. Cybercriminals would still be able to operate as freely as before, but law-abiding businesses have one less tool in their toolbox. Consider the potential dilemma of a health care institution dealing with a particularly unscrupulous advanced persistent threat (APT) group. Suppose the threat actors have infiltrated multiple hospitals and encrypted systems that provide life-saving care to thousands of people. They will not relent without a ransom payment. Do the patients die for the sake of complying with the regulation?

While this example is an extreme case, it is not without precedent.[21] Adversaries target hospitals and health care agencies for multiple reasons, including the life-and-death nature of their work. While a blanket ban on ransomware payments may seem like an obvious solution, implementing one could potentially result in life-threatening scenarios. The criminals will continue their operations, but their victims may have to choose between violating the law or saving lives.

A "no negotiations" approach has other unintended consequences as well. Law enforcement agencies often gather valuable intelligence on cybercriminals through monitoring financial transfers and communications between attackers and their targets. Extended contact with threat groups can lead to cybercriminals making missteps that law enforcement can capitalize upon.

Another important factor when considering new regulations is how they may be abused by threat actors. For example, the Securities and Exchange Commission passed a rule that "material" cyber incidents must be reported on Form 8-K within four business days.[22] Shortly after this declaration, the Black Cat threat group filed a complaint with the SEC claiming one of the businesses they breached was failing to report their compromise.[23] For threat groups, the SEC rule quickly became another way attackers could try to leverage money out of victims. Regulators should be aware that bad actors will study any new rules and weaponize them if possible.

When Regulations Become Gatekeeping

Regulations following a "build from the floor up" approach will foster an economic climate in which innovation is not stifled. Again, this method means new regulations broadly and gently address known problems without significantly impacting business operations. If regulations place too heavy a burden upon businesses, many startups will fail to gather the capital needed to launch. The result will be less innovation, fewer businesses, and, by extension, fewer employment opportunities.

This logic also applies to cybersecurity-related fines. Consider some of the impacts of the EU's General Data Protection Regulation (GDPR) that are seldom discussed. Violations of the GDPR can result in fines including:

- **Less Severe Violations:** Up to 10 million euros ($10.1 million) or up to 2% of a company's total global turnover from the previous year, whichever is higher.[24]
- **Severe Violations:** Up to 20 million euros or up to 4% of the company's total global turnover from the previous year, whichever is higher.[25]

Bearing this in mind, the average U.S. startup launches with $15 million in seed money.[26] By their Series A funding, they average around $42 million. This means a single, minor, infraction of the GDPR, if enforced to its statutory maximum, could be sufficient to destroy these companies before they get off the ground.

What does a minor violation of the GDPR look like? Here are a few examples:[27]

- Collecting any information from a child, who is under the age of 16 years, without parental consent
- Storing, collecting, or processing additional information to identify a user further when it is no longer needed for the user identification
- Failing to follow the basic privacy by cookie protocols
- Hiding the usage of third-party involvement in the privacy policy
- Not keeping records of personal information taken from the users
- Not appointing a responsible person to guide by all the rules of GDPR and keep track that everyone follows it

If a growing startup employing dozens of people makes any of the above mistakes, the GDPR fine could set them back severely. Some argue that this is as it should be. Yet, if a company has fewer than 50 employees, how likely are they to have "a responsible person to guide by all the rules of GDPR and keep track that everyone follows it?"[28]

This legislation places a greater burden upon the shoulders of small and medium businesses (SMBs). The FAANG companies (Facebook, Amazon, Apple, Netflix, and Google) can easily afford to hire GDPR

legal specialists and massive teams to monitor data security. They can build internal systems that ensure no personally identifiable information is stored after it is no longer needed. The same is not necessarily true for small and midsize businesses or startups. A regulatory fine that is a minor irritation to Amazon represents an existential threat to a smaller business.

When regulatory fines and requirements push smaller competitors out of the market, they function as gatekeepers, not safeguards. Equitable cybersecurity regulation should impact organizations of all sizes equally. It should apply just enough positive or negative reinforcement to nudge organizations toward improving their security posture. If it kills any business with a market cap less than $100 million, it is suppressing innovation and imposing a barrier to entering the market.

To frame this issue with a real-world example, when the Lockbit threat group stole 7 terabytes of data from the Capital Health hospital network, it sought a ransom of $250,000.[29] The smallest single infraction of the GDPR could cost Capital Health up to $10+ million. If the goal is to get health care companies to view cyberthreats as a greater threat than regulatory compliance, the incentives seem to be reversed.

Another thing to consider is the large-scale repercussions that naturally follow a data breach. Businesses suffering a breach generally suffer an immediate financial loss. This may be due to the nature of the crime, the expense of recovery operations, and any potential civil litigation that arises as a result of the breach by damaged parties. Their brand reputation is publicly tarnished, and they lose customer trust. Employee morale is harmed, and they may lose personnel. They may also need to raise prices to offset the cost of the breach, making them less competitive in the marketplace.[30] Levying heavy fines on top of these already drastic consequences may prove to be more punishment than many businesses can withstand.

Streamline and Clarify Communications

Governments could benefit by appointing one agency or group to address and communicate cybersecurity policy, concerns, and news. In the United States there is some confusion over which entity is actually "in charge" of cybersecurity issues.

For example, the Cybersecurity and Infrastructure Security Agency (CISA) is tasked with protecting national infrastructure.[31] The National Institute of Standards and Technology (NIST) produces and updates federal information security standards.[32] The SEC recently passed regulations governing the

A person walks into the entrance of the Eindhoven University of Technology, which suspended online activities due to a cyber attack on Jan. 12, 2025 in the Netherlands. (Rob Engelaar / ANP /AFP via Getty Images)

reporting of "material" cyber incidents.[33] Former President Joe Biden's Executive Order 14028 tasked various agencies with evaluating and improving the nation's cybersecurity.[34] It is difficult for businesses to know who to collaborate with when multiple public entities are pushing forward with their own visions for cybersecurity.

This structural problem evolved with the creation of multiple government agencies to oversee specific aspects of commerce and public life. Each agency proposing new cybersecurity rules does so within the context of its mission. But these can lead to unintended consequences for areas outside of the agency's purview. Creating a central cybersecurity authority to create and enforce policies would simplify collaboration and eliminate the problem of individual agencies writing regulations specific to their interests. Unfortunately, agencies historically often have been unwilling to relinquish authority.

This dynamic can be observed in discussions surrounding the efforts to create of a Cyber Force branch within the Department of Defense.[35] Currently each branch of the U.S. military has its own internal cybersecurity units, with the Army, Navy, Air Force, and Marines each spending considerable sums to find, recruit, train, and retain their own cybersecurity experts. This has caused some to ask if it might be more efficient to have a Cyber Force within the DoD that serves all branches. Yet, no branch of the military is interested in losing its cybersecurity personnel (or budgets), so the proposal faces strong opposition.[36]

A similar resistance to a unified cybersecurity authority among civilian agencies makes it difficult for governments to create incentives for cybersecurity businesses to improve practices. It would be simpler for private businesses and organizations to parley and collaborate with a singular, authoritative agency speaking for cybersecurity. When potentially hundreds of agencies can create unilateral rules at will, there is no structure for collectively advancing security. Instead of one authority leading cybersecurity toward a specific goal, there are hundreds of proverbial foot soldiers, each attacking the nearest problem in sight. This is not how battles are won.

U.S. Rep. Andre Carson (D-IN) holds up the annual threat assessment during an annual worldwide threats assessment hearing at the Longworth House Office Building on March 26, 2025 in Washington, DC. (Kayla Bartkowski / Getty Images)

If creating a singular agency to deal with cybersecurity issues is not feasible, perhaps appointing a council that reviews regulatory proposals from all government agencies would suffice. Each new cybersecurity regulation would send their proposals to this council that could allow private companies to offer feedback and raise concerns with the upcoming regulation. This creates another step in the process of passing cybersecurity regulations, but it also establishes a venue for collaboration and discussing wide-ranging impacts of legislation.

Building Trust

If the public sector wishes to collaborate and create cybersecurity incentives for the private sector, mutual trust is essential. Both parties must reach a point where they believe the other side is exclusively focused on improving cybersecurity. During tough times, there is a tendency for organizations and agencies to deflect responsibility, create excuses, and place blame elsewhere. These behaviors, while understandable, can quickly erode years of trust-building.

One complex issue affecting mutual trust arises from the duality of government interests in cybersecurity. Some government agencies are sincerely beating the drum for hardening technology against cyberattacks.[37] Other departments and agencies, particularly those dealing with intelligence-gathering and warfare, see exploiting technology as a valuable tool.[38] These organizations have a vested interest in breaking into the technology of others. It is vital for any public agency seeking to influence cybersecurity in the private sector to be autonomous from those that actively cultivate cyberattack capabilities.

Consider the mixed messaging around conversations about the Pegasus program, which some consider to be spyware.[39] The spyware label is misleading, as this tool used to hack and monitor iPhones is openly advertised as a service by the NSO Group.[40] Their customers are primarily national governments.[41] While the NSO Group claims that Pegasus is used only to assist with fighting crime, journalists have reported it is used to persecute reporters, activists, and members of opposition parties.[42] The U.S. government put the NSO Group on a blacklist in 2021, but Pegasus is still accepted in the European Union.[43, 44] If private organizations cannot be sure that their partners in government truly want better cybersecurity, they may resist joining collaborative efforts or sharing internal information.

The private sector prefers robust cybersecurity, as it derives no benefit from operating on vulnerable platforms. Those businesses need public partners who are transparently committed to the same goal. Therefore, it is vital that public partners crafting cybersecurity regulations remain separate and autonomous from departments employing or researching cyberattacks.

Regulators must remember that private companies are ill-equipped to withstand the attacks of nation-states. Some of the largest names in software and cybersecurity have been breached by state-backed threat groups.[45] In these cases, it makes little sense to punish victim organizations for a breach. Just as private security forces are unable to stop an army, private businesses are unlikely to fend off cyberattacks from nation-state actors. Maximum leniency should apply in cases where organizations put forth a good-faith effort to protect their infrastructure but are breached by nation-state actors.

Begin with Broad Goals

As noted earlier, cybersecurity is a fast-moving field, while government operations are intentionally deliberate and thoughtful. Therefore, it makes sense to keep any new regulations/incentives broadly defined to ensure they remain widely applicable as technology advances. The more specific an incentive becomes, the higher the risk that it will become quickly outdated. For example, if an incentive rewards companies for buying a specific type of security hardware, businesses will comply. If later that hardware is found to be vulnerable (or new attacks render it irrelevant), the entire exercise becomes a sunk cost.

People generally think of cybersecurity in terms of network and endpoint protection. Yet, regulations that make sense for securing a workstation may not apply to operational technology, internet-connected devices, cloud services, and so on. This is why new regulations need to take a big-picture approach and set forth broadly applicable rules.

For example, consider incentivizing data protection in the broadest terms possible. One way to begin this process is by stating a measurable goal. Writing regulations is best left to legal professionals, but thinking through the process can be useful for illustrating the point. Suppose the goal is to incentivize businesses to ensure all sensitive data to have quantifiable protection that prevents its misuse. By plainly stating this goal, it becomes easy to enumerate what must be accomplished:

1. Protect data from anything other than its intended use
2. Have measurable safeguards
3. Include carrot/stick incentives for compliance

This broad approach makes it widely applicable across industries and technologies. What are some well-known safeguards used today to protect data?

- Passwords
- Encryption
- Data loss prevention platforms
- Multifactor authentication (MFA)
- Masking
- Tokenization

Under this theoretical high-level rule, a company handling sensitive data would be compliant if they implement one or more common safeguards. They also have the freedom to find equally effective data protection techniques and implement those instead. This allows businesses to choose an approach that aligns with their processes rather than forcing them down a particular path.

If the government prefers particular safeguards to others, the incentive structure can be written to accommodate them. For example, suppose the government wants businesses to adopt MFA and encryption over alternative approaches to data security. In this case the hypothetical proposal could be modified to cover the following bases:

1. Organizations handling sensitive data need to implement safeguards to protect it from misuse.
2. These protections must be measurable, effective, and apply to data at rest, in motion, and during processing.
3. Acceptable protective measures include passwords, encryption, MFA, masking, tokenization, and DLP technologies.
4. Those implementing MFA and data encryption will receive a tax break.
5. Those found storing, transporting, or processing sensitive data without using any safeguards will be fined.

While the creation of actual regulations involves a more complex process, this thought experiment provides a rough outline for its successful navigation. Begin with a simple goal, such as incentivizing businesses to secure sensitive data. Offer organizations multiple paths to success while encouraging preferred outcomes with some form of reward. Ensure the regulation broadly applies to endpoints, networks, cloud services, internet-connected devices, smart phones, and so on. This simplistic example demonstrates the concept of building from the floor up: Start with a specific security goal, incentivize desired outcomes, and ensure the goal is widely applicable.

Final Thoughts

There are a number of nontechnical challenges that make it difficult for the government to create effective incentives for cybersecurity. These include a lack of a central cybersecurity authority, competing priorities among agencies, and the inability to predict how new regulations will ultimately impact the private sector. The rapid pace of technological evolution also poses problems for public institutions that (necessarily) work in a deliberate and collaborative fashion. Yet, the current approach of allowing market forces to dictate the cybersecurity landscape alone has resulted in an atmosphere in which threat actors are increasingly active and successful.

Legislation that punishes a company for cybersecurity breaches represents a quick-fix approach, but this also massively disadvantages SMBs and startups. Large fines can put an undue strain on businesses that are already likely to go bankrupt within six months of a successful cyberattack.[46] While large tech firms can

House Democrats hold a press conference Feb. 6, 2025, at the U.S. Capitol on the Taxpayer Data Protection Act in response to Elon Musk's gaining access to the Treasury Department's payment system. (Kayla Bartkowski / Getty Images)

afford significant penalties, smaller businesses that drive innovation and create new markets cannot.

Providing public services and resources is a better approach for impacting the direction of cybersecurity in the private sector. The cybersecurity field relies on several open-source tools and resources to perform critical tasks. If the government lent its knowledge and expertise to existing cybersecurity projects or provided its own, it would naturally attract a following. Some successful examples of this approach include the NIST CSF 2.0 framework and the CISA Known Exploited Vulnerabilities Catalog.[47, 48]

Along the same lines, the government can encourage adoption of strong security principles by structuring the tax code to incentivize the adoption of applicable technologies. Multiple government entities have endorsed zero trust security practices for themselves and their vendors. While the exact definition of zero trust is debated, its core tenets include:

- Identity-based access controls
- Continuous verification
- Least privilege access
- Assumption of breach

If the public sector wants the private sector to adopt similar technologies, then making them less expensive for businesses to adopt will help. Perhaps allowing businesses to leverage their investments in these technologies as a tax write-off would be a good start.

Sharing cybersecurity information can also influence how the private sector behaves. Large technology companies regularly alert their users to security issues or ongoing threats as a matter of maintaining trust

and transparency with their customers. However, the information contained in their announcements is often limited to how their customers are affected or impacts on their product line. Governments, which have access to vast amounts of data the private sector does not, could perform the same function by releasing cybersecurity information that benefits all citizens.

For example, the government could regularly share information about threat groups leveraging particular tactics, techniques or procedures that may affect the public. This would benefit citizens as well as the private sector, who would have access to new threat data. It is quite likely the private sector will quickly find a way to ingest government cybersecurity insights and use this information to improve commercial security services.

Cybercriminals and APTs present a common threat to every legitimate organization's interests. The more quickly public and private sector organizations overcome obstacles hindering collaboration, the better. As Benjamin Franklin once said, "We must all hang together, or, most assuredly, we shall all hang separately." This certainly rings true today, as public and private organizations work to protect themselves from external cyberthreats.

Maxime Lamothe-Brassard began his cybersecurity career at the Canadian Department of National Defense before providing direct assistance to organizations facing cyber defense challenges. His distinguished career includes key roles at CrowdStrike and Google, as well as being part of Chronicle Security's founding team, ultimately leading him to establish LimaCharlie to revolutionize security operations infrastructure.

Endnote

1 Petrosyan, A. (2024, July 30). Estimated cost of cybercrime worldwide 2018-2019. Statista. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

2 Ewing, G., & Jodka, S. H. (2024, July 31). But really, what cybersecurity requirements and standards does my company need to follow and why?. Reuters. https://www.reuters.com/legal/legalindustry/really-what-cybersecurity-requirements-standards-does-my-company-need-follow-why-2024-07-31/

3 Checkpoint. (2024, July 16). Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks. Checkpoint. https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks

4 Suarez, J., & Curry, B. (2025, February 3). The top 10 cybersecurity companies in the United States. Fortune. https://fortune.com/education/articles/top-cybersecurity-companies/

5 Moran, L. (2023, December 18). Regulatory compliance tops risk concerns for GCs, report finds. Legal Dive. https://www.legaldive.com/news/regulatory-compliance-tops-risk-concerns-for-gcs-report-finds/702860/

6 Allianz. (2024, January 16). Allianz Risk Barometer: Identifying the major business risks for 2024. https://www.allianz.com/en/economic_research/insights/publications/specials_fmo/2024_01_16-Allianz-Risk-Barometer.html

7 Institute of Data. (2024, June 7). Compliance vs Security in Cyber Defense: Successfully Navigating the Intersection. https://www.institutedata.com/us/blog/compliance-vs-security-in-cyber-defense-successfully-navigating-the-intersection/

8 Toulas, B. (2024, July 13). Hackers use PoC exploits in attacks 22 minutes after release. Bleeping Computer. https://www.bleepingcomputer.com/news/security/hackers-use-poc-exploits-in-attacks-22-minutes-after-release/

9 National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. (Department of Commerce, Washington, D.C.), Cybersecurity White Papers (CSWP) 29. https://doi.org/10.6028/NIST.CSWP.29

10 Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). Known Exploited Vulnerabilities Catalog. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

11 Roth, F., & Patzke, T. (2025, February 12). About Sigma. Sigma Documentation. https://sigmahq.io/docs/guide/about

12 Devoteam. (n.d.). Unveiling the AI-powered cybersecurity guardian: A deep dive into the evolution of VirusTotal. https://www.devoteam.com/expert-view/virustotal-threat-analysis/

13 Imperva. (n.d.). Metasploit. Thales. https://www.imperva.com/learn/application-security/metasploit/

14 Cloudflare. (n.d.). What is OWASP? What is the OWASP Top 10?. https://www.cloudflare.com/learning/security/threats/owasp-top-10/

15 CISCO. (n.d.). How TheHive Project and Cisco Security work togther. https://www.cisco.com/c/en/us/products/security/technical-alliance-partners/hive-project.html

16 Yeti. (n.d.). What is Yeti?. https://yeti-platform.io/

17 Patrizio, A. (2024, February 6). 20 free cybersecurity tools you should know about. TechTarget. https://www.techtarget.com/whatis/feature/17-free-cybersecurity-tools-you-should-know-about

18 Kressin, J. (2024, February 7). Hall of Fame: Linus Torvalds. Search Guard. https://search-guard.com/blog/hall-of-fame-linus-torvalds/

19 RunCloud. (2024, November 21). 9 Best Linux Distros in 2024. https://runcloud.io/blog/best-linux-distros

20 Marks, J. (2021, May 21). The Cybersecurity 202: Cybersecurity pros are split on banning randomware payments. The Washington Post. https://www.washingtonpost.com/politics/2021/05/21/cybersecurity-202-cybersecurity-pros-are-split-banning-ransomware-payments/

21 United Nations Security Council. (2024, November 8). Ransomware Attacks on Healthcare Sector 'Post a Direct and Systemic Risk to Global Public Health and Security', Executive Tells Security Council. UN. https://press.un.org/en/2024/sc15891.doc.htm

22 U.S. Security and Exchange Commission. (2023, July 26). SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies [Press release]. https://www.sec.gov/newsroom/press-releases/2023-139

23 Hill, M. (2023, November 16). BlackCat/APLHV ransomware gang files SEC complaint over victim's "undisclosed" data breach. Cyber Security Hub. https://www.cshub.com/attacks/news/blackcataplhv-ransomware-gang-files-sec-complaint-over-victims-undisclosed-breach

24 Art. 83 GDPR – General conditions for imposing administrative fines - General Data Protection Regulation (GDPR). (2018b, March 29). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-83-gdpr/

25 Art. 83 GDPR – General conditions for imposing administrative fines - General Data Protection Regulation (GDPR). (2018b, March 29). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-83-gdpr/

26 Kruze Consulting. (2024, August 26). Startup Valuations in 2024. Kruze consulting Blog. https://kruzeconsulting.com/blog/startup-valuations/

27 CookieScript. (2022, April 1). What are the GDPR violations that lead to fines? https://cookie-script.com/knowledge-base/what-are-gdpr-violetion-that-lead-to-fines

28 CookieScript. (2022, April 1). What are the GDPR violations that lead to fines? https://cookie-script.com/knowledge-base/what-are-gdpr-violetion-that-lead-to-fines

29 Paganini, P. (2024, January 9). LockBit ransomware gang claims the attack on Capital Health. Security Affairs. https://securityaffairs.com/157170/cyber-crime/lockbit-ransomware-hit-capital-health.html

30 Schuman, E. (2024, December 4). 63% of companies plan to pass data breach costs to customers. CSO Online. https://www.csoonline.com/article/3616501/63-of-companies-plan-to-pass-data-breach-costs-to-customers.html

31 About CISA | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/about

32 About NIST | NIST. (2022, January 11). NIST. https://www.nist.gov/about-nist

33 Gerding, E. (2023, December 14). Cybersecurity Disclosure. U.S. Security and Exchange Commission. https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-disclosure-20231214

34 Executive Order 14028, Improving the Nation's Cybersecurity | NIST. (2022, July 11). NIST. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

35 Pomerleau, M. (2024, March 25). US must establish independent military cyber service to fix 'alarming' problems — report. DefenseScoop. https://defensescoop.com/2024/03/25/u-s-must-establish-independent-military-cyber-service-or-risk-catastrophic-condition-report/

36 Munk, C. W. (2024, November 29). The Case for and Against Creating a Military Cyber Force. The Wall Street Journal. https://www.wsj.com/tech/cybersecurity/creating-military-cyber-force-75844bf5

37 Cybersecurity | Homeland Security. (2021, November 16). U.S. Department of Homeland Security. https://www.dhs.gov/topics/cybersecurity

38 Office of the Director of National Intelligence National Counterintelligence and Security Center. (2024). National Counterintelligence Strategy 2024. https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf

39 Amnesty International. (2023, August 10). Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally. https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

40 Response from NSO Group to the Pegasus Project. (2021, July 18). The Washington Post. https://www.washingtonpost.com/investigations/2021/07/18/nso-group-response-pegasus-project/

41 The Pegasus Project. (2021, July 18). OCCRP. https://www.occrp.org/en/project/the-pegasus-project

42 Amnesty International. (2023a, August 10). Forensic Methodology Report: How to catch NSO Group's Pegasus. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

43 Kirchgaessner, S. (2021, November 3). Israeli spyware company NSO Group placed on US blacklist. The Guardian. https://www.theguardian.com/us-news/2021/nov/03/nso-group-pegasus-spyware-us-blacklist

44 Roussi, A. (2022, June 22). Pegasus used by at least 5 EU countries, NSO Group tells lawmakers. POLITICO. https://www.politico.eu/article/pegasus-use-5-eu-countries-nso-group-admit/

45 Microsoft Threat Intelligence. (2023, September 14). HAFNIUM targeting Exchange Servers with 0-day exploits. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

46 PCI Compliance: What to know about digital Payment Security. (2020, May 12). Verizon Enterprise. https://www.verizon.com/business/resources/articles/small-business-cyber-security-and-data-breaches/

47 National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. (Department of Commerce, Washington, D.C.), Cybersecurity White Papers (CSWP) 29. https://doi.org/10.6028/NIST.CSWP.29

48 Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). Known Exploited Vulnerabilities Catalog. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

A staff member demonstrates the e-CNY payment system during the 2024 China International Fair for Trade in Services in Beijing. (Li Xin / Xinhua via Getty Images)

Implications of Alternative Payment Methods in a China-Taiwan Confrontation

Gavin Moore

Introduction

In March 2024, former U.S. Indo-Pacific Command Adm. John Aquilino testified to the Senate Armed Services Committee that "all indications point to the PLA (the People's Liberation Army) meeting President Xi Jinping's directive to be ready to invade Taiwan by 2027."[1] Aquilino's assertion was based on the PLA's buildup "occurring across land, sea, air, space, cyber and information domains" on a scale "not seen since World War II."[2] At the time of writing, forecasters have given an 8.6 percent probability of a lethal confrontation occurring between China and Taiwan before Oct. 1.[3] The prospect of China invading the island – potentially on a shorter timeline than Xi's directive – is one U.S. policymakers must take seriously.

How can we cut through the noise and make sense of the timing of a possible confrontation between China and Taiwan? Analysis and attention have reasonably focused on the actions of the PLA and the "anaconda strategy."[4] However, the impact of warfare plays out across many sectors, including some that may appear indirectly related to the conflicts themselves. Witness the worldwide volatility in the price of sunflower oil[5] [6] after the Russian invasion of Ukraine in February 2022 or the impact on international trade of al-Houthi rebels

targeting oil tankers in the Red Sea in September 2024.[7] While these events occurred after conflict had begun, we can look for early warning signals that would indicate a China-Taiwan confrontation is more likely to occur.

One such signal is China's role in the development of alternative payment methods (APMs). APMs are defined as financial modalities, including payment, settlement and reserve holdings, that either take place outside of Western financial institutions, such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) or are performed without the use of the U.S. dollar (USD) as the main currency of transaction. This includes the use of other fiat currencies like the Chinese renminbi (RMB), as well as the use of digital currencies, like cryptocurrencies or Central Bank Digital Currencies (CBDCs).[8]

A Pivot in China's APM Strategy

China's APMs strategy to date has focused on undermining USD hegemony through a process of diversifying its own position, for example by buying up more gold over the previous decade to reduce reliance on USD in its reserves. Despite this, China is the world's largest foreign exchange holder, with $3 trillion of its reserves in a foreign currency, a majority of which is in USD.[9] Holding USD in reserve has made sense from an international trade perspective for China: USD reserves make trade easier to execute, as the dollar's hegemony means most trading continues to take place in dollars. Nonetheless, China has also made great efforts to promote the RMB[10] among its allies and trading partners, for example by incentivizing the use of RMB in crude oil transactions.[11,12]

Policymakers should be alert to a potential pivot in China's APMs strategy as an early warning signal of a possible China-Taiwan confrontation. Rather than diversifying holdings or promoting RMB, China's APMs strategy is becoming more targeted, using de-dollarization[13] to blunt the effectiveness of U.S. economic sanctions. This strategic pivot has been spurred by the events following Russia's invasion of Ukraine in 2022. During the conflict, we have seen a noticeable acceleration in the development of APMs by both Russia and China for the purpose of blunting sanctions, although with some subtle and crucial differences. Russia's approach can be viewed as rapidly reactive to an unprecedented level of economic sanctions from Western governments, while China has been cautiously proactive, laying the groundwork in anticipation of future sanctions should it invade Taiwan, but not yet embracing APMs with the same enthusiasm as Russia.

As China pivots its APM strategy, U.S. policymakers will need to consider the implications of this for (a) maintaining USD's position as the world's reserve currency,[14] a key part of President Donald Trump's election policy platform,[15] and (b) the effectiveness of sanctions as a foreign policy lever in the event of an invasion of Taiwan. A priority among several recommended actions for this administration would be the creation of an APM Strategic Coordination Unit to monitor early warning signals that would point to an increased probability of an invasion. The unit's remit would be to ensure information-gathering and rigorous scrutiny of these signals, and to serve as a convening body for departments, working groups , and agencies across government. This will ensure the U.S. is unified, coordinated, and prepared to respond to APM developments that would indicate an increased probability of invasion.

APM Landscape After Russia's Invasion of Ukraine

Following Russia's invasion of Ukraine in February 2022, the level of economic sanctions imposed by Western governments has been described as unprecedented and is significantly above those imposed following Russia's 2014 occupation of Crimea. Since the more recent invasion, over 18,300 sanctions designations have been made against individuals, entities, vessels, and aircraft with ties to the Russian state.[16] Sanctions have not been limited to Russian targets either, with the U.S.'s "secondary sanctions" regime[17] targeting Chinese firms supplying "dual use" items,[18] as well as firms with direct involvement in arms supplies to Russia's war effort.[19]

The Russian and Chinese response to these sanctions has shifted the APMs landscape in a way that U.S. policymakers may look back on as a turning point in efforts to de-dollarize the international financial system. Of course, de-dollarization itself is not a novel

concept.[20,21,22] Predictions of the impending demise of the USD as the world's pre-eminent currency have a long history[23] and have regularly made the predictors look foolish.[24,25] So why might this time be different?

Changes in Russia's Approach to Digital Assets

As recently as January 2022, the Central Bank of Russia had been pushing for a complete ban on cryptocurrencies, with support from the Russian Security Services.[26] The situation now couldn't be more different. Cryptocurrencies have become part of the war effort, with Russia reportedly using crypto to pay for dual use goods from Chinese companies due to sanctions causing difficulties in transacting in rubles.[27] Pro-Russian groups with links to the state have also been raising crypto donations for the state's war effort,[28] although the amount of crypto that has been raised has been vastly exceeded by crypto donations to Ukraine.[29]

The Russian government enacted two crypto-related bills on international payments and mining in August 2024,[30] and Russian lawmakers – like their U.S. counterparts – are considering a Bitcoin national reserve.[31] Russia has also accelerated development of its own CBDC, referred to as the "robot ruble." In October 2024, the Central Bank of Russia revealed a mass rollout date for the currency by July 1, 2025, although there were reports of pushback by retailers[32] and slower-than-anticipated uptake by banks during a pilot program.[33] There are also rumors the Central Bank of Russia plans to use tokenized assets, such as gold and other commodities, on Russia's alternative to the SWIFT payment platform.[34] This rapid pivot in its APMs strategy was encapsulated in July 2024 by President Vladimir Putin, who called cryptocurrencies "a very dynamic and promising direction of the modern economy." [35]

This embrace of digital assets – whose timeline parallels the Russian invasion of Ukraine – is clearly an attempt to negate the effectiveness of Western sanctions by reducing Moscow's reliance on Western financial institutions.

Russian Alternatives to SWIFT

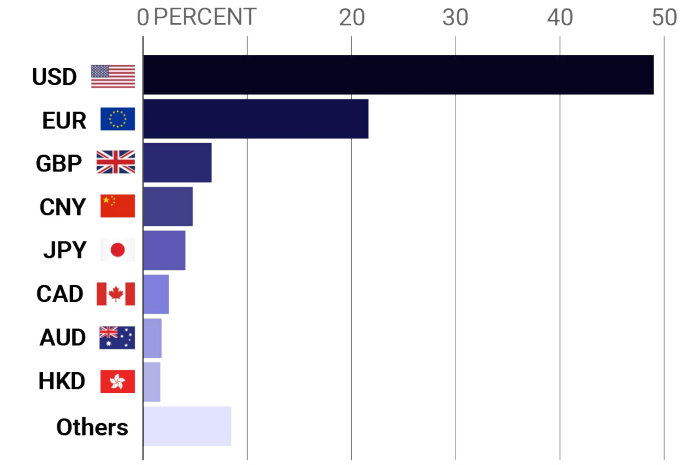
Recent sanctions are also impacting Russia's desire to develop an alternative to SWIFT. Take the global payment network as a case study. Created in 1973, SWIFT has long been the "global financial artery" that allows the smooth and rapid transfer of money across borders.[36] SWIFT links 11,000 banks and institutions in more than 200 countries and sends more than 40 million messages a day as trillions of dollars change hands. The USD dominates payments on SWIFT, which accounts for around 49 percent of the system's payments, compared to 4.7 percent for the yuan.[37]

The USD's historic dominance of SWIFT has been challenged by Russian and Chinese alternatives, both of which predate Russia's invasion of Ukraine. Russia developed the System for Transfer of Financial Messages (SPFS) in 2014 after the U.S. and its allies threatened it with expulsion from SWIFT because of its invasion of Crimea – a threat they made good on in March 2022 following the full-scale invasion of Ukraine.

The success of these SWIFT alternatives has, until now, been mixed. The use of SPFS has reportedly tripled in 2023 since 2022,[38] although Russia has had little alternative following its expulsion from SWIFT. In any event, this growth in the use of the SPFS is starting from a low base.[39] Only a fraction of organizations and countries are operating on SPFS compared to SWIFT. In June 2024, the EU outlawed the use of SPFS by EU entities operating outside of Russia,[40] which is likely to curtail any further growth of the platform. Russia

Currencies of SWIFT

Shares processed on global payment network SWIFT



Source: Statista

APMs of BRICS

BRICS Cross-Border Payments Initiative (BCBPI)	A voluntary and non-binding initiative that aims to strengthen corresponding banking networks within BRICS and enable settlements in local currencies of BRICS members. Seen as a potential alternative to SWIFT and sometimes referred to as BRICS Pay.
BRICS Bridge	Inspired by mBridge (see below), the BRICS Bridge aims to let countries conduct cross-border settlements using digital platforms runs by BRICS members' central banks, including a combination of CBDCs, blockchain, and tokens.
BRICS Clear	An independent securities depository and settlement system available only to BRICS members and seen as an alternative to Western entities such as the Depository Trust and Clearing Corporation and Euroclear.
mBridge (outside of BRICS)	Coordinated by the Bank for International Settlements, mBridge is a collaboration between the central banks of the UAE, China, Hong Kong and Thailand. mBridge is a platform that allows for real-time, cross-border payments and foreign exchange transactions using CBDCs.

Source: Gavin Moore

knows that it cannot go it alone; the success of a SWIFT alternative relies on convincing other countries.

Enter BRICS

The BRICS[41] countries are geographically dispersed across three continents. They seek cooperation on a diverse and growing range of priorities that often conflict with the West. They are ambitious about expansion to include more members, and they are pushing for further institutionalization as a counterweight to the IMF and World Bank. In January 2024, BRICS saw the accession of four new countries, the largest expansion in the organization's history. The addition of Egypt, Ethiopia, Iran, and the United Arab Emirates takes the bloc's share of global gross domestic product (at purchasing power parity) from 32 percent to 36 percent and population from 41 percent to 46 percent.[42] A further 13 countries were offered partnership status at an October 2024 summit in Kazan, Russia.[43]

Until now, BRICS has been united more in what it opposes than in what it supports. While BRICS members have considered APMs initiatives before, like the New Development Bank and BRICS Bridge, proposals at the 2024 Kazan summit[44] represent a significant acceleration in the institutionalization of APMs among its membership. This was most evident in proposed alternatives to SWIFT such as the BRICS Cross-Border Payments Initiative (BCBPI).

Initiatives like BCBPI are being driven by Moscow,[45,46] but the motivation behind the latest SWIFT alternative is primarily as a means of avoiding economic sanctions rather than challenging USD hegemony. In Putin's post-summit news conference, he called the Kazan Declaration "a comprehensive conceptual document" that "reaffirms the commitment of all BRICS countries to building a more democratic, inclusive, and multipolar world order" and "underscores our collective determination to oppose the practice of imposing unlawful sanctions and attempts to erode traditional moral values."[47] The West's sanctions response to the invasion of Ukraine is clearly a significant motivating factor in Russia's recent APMs push multilaterally.

BRICS members who continue to rely on SWIFT and are not subject to U.S. sanctions now, or would not anticipate being subject to sanctions in the future, are less enthusiastic about the proposal and may have different goals.[48] In August 2023, South African Finance Minister Enoch Godongwana said BRICS would not be looking to replace international payment systems like SWIFT but that a BRICS payment system is instead important for "strengthening trade" in local currencies.[49]

The effectiveness of these SWIFT alternatives and their impact on the USD's status as the world's reserve currency remains to be seen. Nevertheless, the Kazan Declaration does represent a much more sustained APMs drive than we have seen previously. U.S. policymakers will want to monitor concerted attempts by BRICS countries to reduce the overall USD share of global reserves. They will also want to pay close attention to any shifts in Moscow's APMs strategy, for example, if the lifting of economic sanctions forms part of a deal to end the war in Ukraine.[50]

China's APMs Strategy

In headline terms, Russia and China's APMs strategies have been on similar recent trajectories in the pursuit of de-dollarization to provide a bulwark against sanctions. But if we scratch beneath this surface, more subtle differences in approach appear.

Raising the Renminbi's Profile

China's initial APMs approach was focused on increasing the use and economic heft of the RMB, a policy that has borne fruit. For instance, the share of RMB in all cross-border transactions of Chinese non-bank entities with foreign counterparts was close to zero in 2010, but by late 2023, this had risen to around 50 percent.[51] In contrast, the USD share in these transactions has declined from around 80 percent in 2010 to 50 percent in 2023.[52] Thanks in part to the development of its own SWIFT alternative in 2015, the Cross-Border Interbank Payment System (CIPS),[53] 25-30 percent of China's goods-and-services trade is now settled in its own currency.

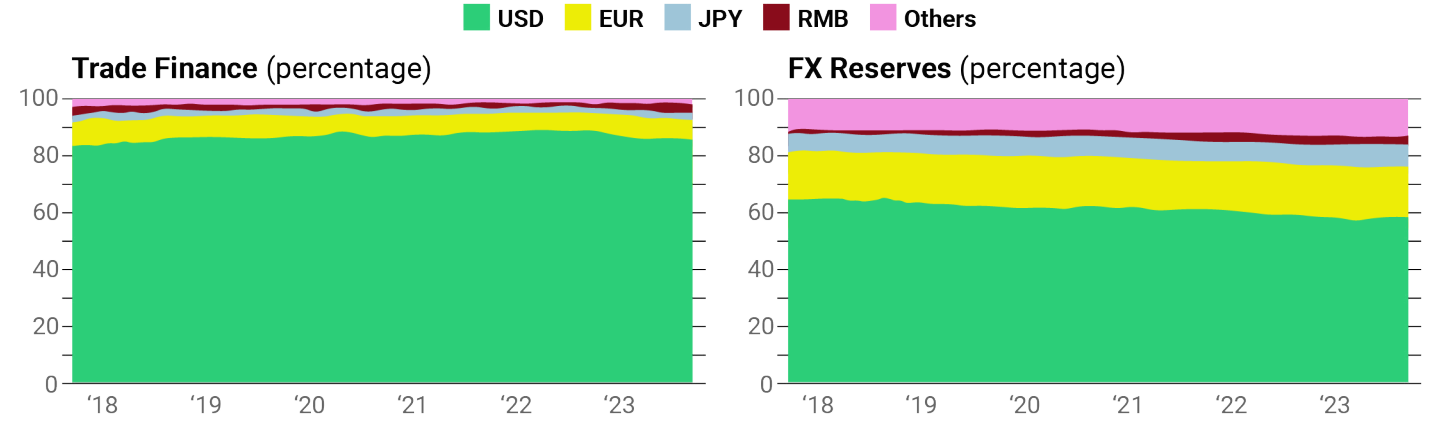
China has been able to leverage the RMB in partnership with countries hit by sanctions, such as Iran and Russia. For example, Iran and China signed a 25-year cooperation plan to facilitate trade in 2022. In May 2023, Russian authorities were reportedly considering using RMB to facilitate their own bilateral trade with Iran.[54] While the RMB is on the rise, it is starting from a low base compared to USD as both reserve currency figures and its use on SWIFT demonstrate.

Like Russia, China's own SWIFT alternative has delivered mixed results. While it has helped to promote RMB in goods-and-services trade, CIPS still relies on SWIFT for translating messages between China and its business partners, with around 80 percent of CIPS payments estimated to use SWIFT messaging systems. This gives the U.S. leverage over private entities that continue to rely on SWIFT and the dollar in their transactions with China.[55] There is scope to grow the influence of CIPS through the recent expansion of BRICS membership. Of the new members, only the United Arab Emirates contains a direct CIPS participant within its borders.[56] China may also look to the 13 countries that received BRICS partner status in Kazan to further expand adoption of CIPS.

China's Complicated History with Digital Assets

China was an early adopter of CBDC technology, gaining an advantage over its counterparts, including

USD Dominance in Global Trade Finance and FX Reserves



Source: IMF

Russia, with the introduction of a digital yuan (e-CNY) in 2014. The digital yuan is directly issued by the People's Bank of China (PBOC) as a digital currency to individuals. Unlike a wholesale CBDC, which is usually intended for banks and financial institutions, the digital yuan is a retail CBDC designed for everyday transactions.[57] It is pegged 1:1 with the physical yuan and does not bear interest. The PBOC reported around 180 million individual wallets in use as of July 2024,[58] assisted by integration into the hugely popular WeChat app.[59]

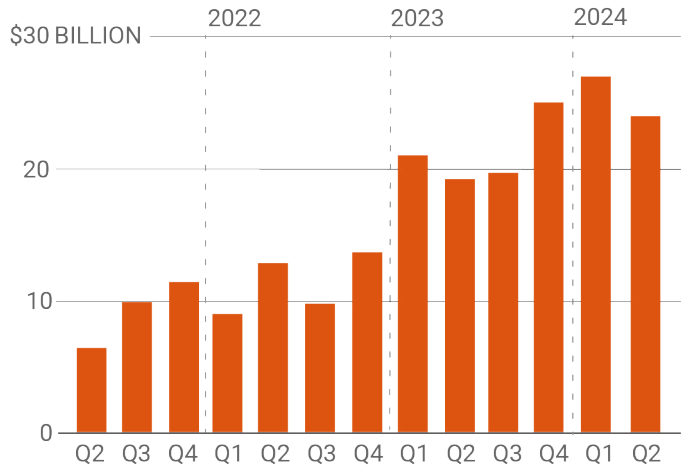
China is also actively seeking to promote e-CNY on the international stage, including on platforms like mBridge,[60] which is built on distributed ledger technology to enable instant cross-border payments and settlement for multiple CBDCs.[61] China was one of the prime movers in building the infrastructure behind mBridge. As a proof of concept, the UAE's central bank sent 50 million in digital dirhams ($13.6 million) to China in a single transaction on the platform in January 2024.[62]

While China has been an enthusiastic proponent of the CBDC technology, this enthusiasm has not extended to cryptocurrencies outside of PBOC control. While cryptocurrency is often perceived to be banned in China,[63] the reality is more complex. In 2017, China banned initial coin offerings and clamped down on exchanges operating from its territory. China's foreign exchange regulator has recently introduced new rules on the country's banks to monitor and flag risky trades involving cryptocurrencies.[64] However, individual holdings and cryptocurrency transactions are not strictly illegal. Despite this, digital currencies do not have the same status as fiat currencies, and digital currency-related business activities were made illegal financial activities in a swath of 2021 restrictions.[65] The PBOC said these measures were necessary as cryptocurrency "seriously endangers the safety of people's assets"[66] due to its highly speculative nature, and for its use in facilitating financial crime.[67] Ironically, China has become the world's second-largest holder of Bitcoin (behind the U.S.), which it has acquired through asset seizures linked to illegal activities.[68]

The perception that it is impossible to transact in cryptocurrencies in China is inaccurate, even if the barriers to entry are high. For example, blockchain

Crypto Exchanges in China

Total value received from select over-the-counter exchanges in China



Source: Chainanalysis

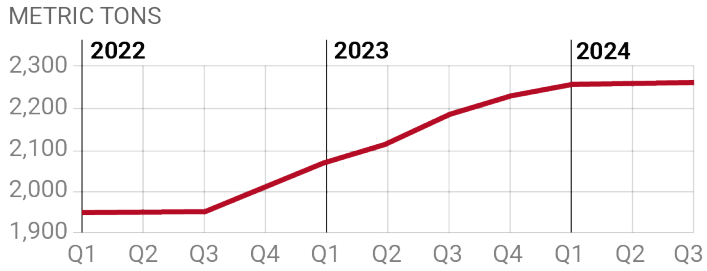
analytics firm Chainalysis' 2024 Global Crypto Adoption Index ranks China as high as 20th out of 151 countries in terms of cryptocurrency adoption (the U.S. is ranked 4th and Russia 7th).[69] As China's economy struggles and the value of the property market declines, wealthy Chinese individuals are increasingly turning to crypto through over-the-counter platforms.

While the rapidly reactive approach to digital assets represent a clear and recent shift in Russian APMs policy, for China the picture is more complicated. Some commentators are suggesting China is taking a "long bet" that payments technology, not a creditors' rebellion or armed conflict, will reduce the power the U.S. gets from being at the center of global finance.[70] But at least at the official level, China has not embraced cryptocurrencies to the same extent Russia has.

China's Cautiously Proactive Strategy

The long-term aim of China's APMs strategy has been to develop a currency order that is less dependent on USD. President Xi Jinping has been critical of the current order and how it has underwritten the use of sanctions. Xi told a BRICS Business Forum meeting in June 2022 that members should oppose "unilateral sanctions and abuse of sanctions, and reject the small

China's Increasing Gold Reserves



Source: World Gold Council

circles built around hegemonism."[71] We may now be seeing signs of a pivot – in alignment with Russia – from promoting the RMB toward providing a bulwark against future possible sanctions.

Take the PBOC's recent gold-buying spree as an example.[72] The PBOC bolstered its gold purchases by 30 percent over the course of 2023.[73] The IMF reports that China's share of gold in total reserves has increased from less than 2 percent in 2015 to 4.3 percent in 2023. During the same period, the value of China's holdings of U.S. Treasury and Agency bonds relative to currency reserves declined from 44 percent to about 30 percent.[74]

China and Russia have not been alone in buying up gold as a reserve asset. However, the share of gold in FX reserves of countries aligned with the United States has been broadly stable. The IMF therefore concludes that "gold purchases by some central banks may have been driven by concerns about sanctions risk."[75] China's gold purchases correspond to the Russian invasion of Ukraine, particularly when economic sanctions began to bite in the third and fourth quarters of 2022, leading some to speculate that China is learning from what happened to Russia in the aftermath.[76]

Despite this acceleration, China remains the world's sixth-largest holder of gold reserves, with Russia fifth and the U.S. first.[77] China's purchases of gold paused when prices reached an all-time high of $2,450 per ounce in July 2024. However, the PBOC has now resumed buying the reserve, reporting its third consecutive monthly gold purchase in January 2025, despite gold prices continuing to rise.[78] There likely is a geopolitical dimension behind the recent gold buying spree.

Some commentators have argued that initiatives like the BCBPI could undermine China's patient efforts to increase the market share of RMB[79] and therefore question the long-term viability of these proposals. However, it is highly unlikely China would have given its backing to the Moscow-led initiatives if they were not serving its strategic interests. This could suggest a cautiously proactive shift in emphasis in China's APMs policy from promoting the RMB first, toward measures that provide a bulwark against future economic sanctions.

We may be seeing further evidence of this in China's contributions to the mBridge platform and how a BRICS Bridge might develop. Putin has been pushing for the BRICS countries to back BRICS Bridge. Coordination of the mBridge platform has been provided by the Swiss-based Bank of International Settlements, of which Russia is not a member. As such, Russia was not part of the original quartet of central banks (China, Hong Kong, Thailand, and the United Arab Emirates) on mBridge.[80] The Bank of International Settlements announced its decision to withdraw from its coordinating role in the mBridge platform in October 2024.[81] It is speculated that the bank withdrew due to fears mBridge could be used to evade sanctions.[82]

As a leading contributor to its technological development, China is now poised to take a leading role on mBridge. Policymakers will want to monitor both how mBridge further develops under China's stewardship (e.g., if the number of central bank participants expand beyond the current quartet) and whether China allows mBridge to be subsumed by BRICS Bridge or maintains the former as a distinct entity outside of Russian influence.

Given that China's APMs strategy on gold, the BCBPI, and mBridge can be interpreted as beginning to build resilience to possible future sanctions in the event of a confrontation with Taiwan, policymakers will want to identify further signals of shifts within its APMs strategy.

Signals That Increase the Probability of a Chinese Invasion of Taiwan

This section looks at further possible early warning signals of a more decisive shift in China's APMs approach toward protecting itself from the impact of future economic sanctions. These should be seen as relatively weak signals, which in and of themselves would not indicate a conflict is imminent and may not appear to be directly linked to a confrontation with Taiwan. This contrasts with something like the PLA's military buildup identified by Aquilino, which we can clearly see as more directly related. However, when viewed as a direction of travel regarding China's APMs strategy, these signals could be part of a much bigger picture, indicating that an invasion is more likely. As such, they deserve greater attention from policymakers.

The following signals and evidence to support them are non-exhaustive. Nevertheless, these illustrative examples give a sense to policymakers of the varied ways in which China's APMs strategy could evolve. The evidence in each case points to potentially key indicators that could be monitored and tracked by the recommended APMs Strategic Coordination Unit explored in the next section.

Deeper integration of BRICS countries

The long-term effectiveness of the APMs specified in the 2024 Kazan Declaration are difficult to assess in the short term. BCBPI and BRICS Clear hold promise of a more sustained effort to move from a dependency on the USD and the Western-led international financial system. Aside from developments at the BRICS institutional level, an early warning signal of a shift in China's APMs strategy could see accelerated efforts by China to leverage its influence over other BRICS members and partners, encouraging them to reduce reliance and usage of USD and move further within the orbit of the RMB and CIPS.

Evidence:

1. New bilateral swap lines between the PBOC and other BRICS members or partners.
2. Additional use of the CIPS within BRICS countries or partner countries.
3. Further regulatory harmonization among BRICS members, such as the realization of BCBPI.

Russian President Vladimir Putin and representatives of 30 countries gather for a photo session during the BRICS Leader's Summit, October 24 2024, in Kazan, Tatarstan Republic, Russia. (Getty Images)

Chinese authorities turn a blind eye to use of non-Know Your Customer (KYC) digital asset exchanges

Chinese government policy limits transactions of cryptocurrencies. Chinese authorities have been vocal in highlighting their crackdowns on illicit crypto activity.[83] However, another early warning signal would see the growing use of non-KYC exchanges in China, which, while still officially illegal, would nonetheless be tolerated by a lack of enforcement action by state authorities. KYC checks are a due-diligence procedure that helps verify the identity backgrounds of customers, clients, and suppliers, reducing the opaqueness of financial transactions and are part of compliance with global anti-money laundering/terrorist financing standards.

There are parallels with the use of the sanctioned Garantex exchange in Russia,[84] which has allowed funds connected to crime and from high-risk services such as mixers (which obscure the origins and identity of crypto funds) and low-KYC checks on its platform. Users of Garantex attempt to use crypto exchanges like these to withhold key information about the transactions of individuals and entities. If the use of non-KYC exchanges in China grows, it could indicate a growing tolerance of these platforms, with the intention of helping entities with links to the state in evading future sanctions.

Evidence:

1. The increased use of Chinese-language marketplaces, such as Huione Guarantee, for illicit activity paid for by cryptocurrencies. Huione Guarantee continues to receive and send funds from Garantex, despite the sanctions imposed on the latter.[85]
2. Blockchain analytics firms like Chainalysis seeing increased transactions on mixers and non-KYC exchanges by users to and from China.

Financial Action Task Force (FATF) downgrades China

The FATF – an intergovernmental organization that sets international standards to prevent money laundering and terrorist financing – regularly reports on each country's efforts to comply with these standards. This reporting is known as the Mutual Evaluation Framework. China's next report is due around August 2026. Any evidence of backsliding from the previous reporting period (2019-2021)[86] based on inadequate regulatory compliance, particularly around its KYC reporting obligations, may indicate an increased willingness to tolerate sanctions evasion activities such as those identified above and a disregard for international financial norms. To note, Russia has been suspended from FATF since February 2023 in response to the invasion of Ukraine.

Evidence:

China's next mutual evaluation report demonstrates a rise of partial compliance or noncompliance with money laundering, terrorist financing and the proliferation of weapons of mass destruction standards determined by FATF.

China removes legislative restrictions to crypto trading in its territories

There are some indications that the Chinese government may enact legislation to "unban Bitcoin" and remove the most restrictive effects of the 2017 and 2021 cryptocurrency legislation.[87] We are already starting to see moves to legitimize the sector. In August 2024, China's supreme court and public prosecutor revised their interpretation of the country's anti-money laundering laws to recognize "digital asset" transactions.[88] Bringing cryptocurrencies into the scope of the law may encourage further adoption as there would be a firmer regulatory underpinning.

There is also speculation that the Trump administration's perceived favorability[89] toward crypto may cause China to rethink its position,[90] such as building a strategic Bitcoin reserve if the U.S. moves first.[91] [92] Trump appears receptive to this issue, responding to a question about a possible U.S. reserve by saying: "We're gonna do something great with crypto, 'cause we don't want China, or anybody else, not just China, others are embracing it, and we want to be the head."[93] A conversion by the Chinese government from crypto-skeptic to crypto-enthusiast may not be too far-fetched, with China taking a long

bet on payments technologies as a lever to undermine the power of the USD.

Looking at Hong Kong may also be instructive. Hong Kong is something like a crypto hub in East Asia, experiencing the largest year-on-year growth of crypto adoption in the region (at 85.6 percent), with regulators' openness and legislative framework fostering this environment.[94] The Hong Kong government announced plans in November 2024 to exempt private equity funds, hedge funds, and other investment vehicles from paying tax on gains from cryptocurrencies,[95] a stark contrast from mainland China's approach. Under the "one country, two systems" model, it is speculated that China may be using Hong Kong to test policies related to crypto.[96] As such, developments the regulatory landscape for cryptocurrencies in Hong Kong could indicate the start of a change in approach in China.

Evidence:

1. Future legislation to reduce the barriers to entry for cryptocurrency use in China and reverse the 2017 and 2021 restrictions or setting up a strategic cryptocurrency reserve.
2. Increased "on-ramping" (conversion of fiat currency to crypto assets) and "off-ramping" (conversion of crypto assets back to fiat) would indicate China is rapidly moving funds out of conventional banking systems.
3. Regulatory initiatives on cryptocurrencies implemented in Hong Kong are "imported" to mainland China.

Sustained re-acceleration of PBOC purchasing of gold or other non-fiat currencies

The PBOC has been increasing its purchases of gold in recent years to diversify reserve holdings away from USD and potentially blunt the impact of future sanctions. While China paused purchases of gold in 2024 when prices hit record levels, the PBOC since reported its third consecutive monthly gold purchase in January 2025. This despite the price of gold exceeding 2024 levels.[97] An early warning signal here would see China continue to significantly increase its gold reserves over a sustained period, potentially tokenizing gold assets as proposed by the Central Bank of Russia, or further diversify to other non-fiat reserves like silver.

Evidence:

1. The World Gold Council reports show a significant uptick in the PBOC's purchasing of gold reserves over a sustained period.
2. The PBOC announces plans to tokenize these gold assets, potentially for use on both mBridge and the BRICS Clear platforms.

A growing number of entities that normally trade in RMB pre-emptively switching to other currencies

China has been moderately successful in increasing the prevalence of the RMB in international financial transactions. However, the RMB's use in payments worldwide remains limited, with its global market share increasing to 2.5 percent as of May 2023, from 1.1 percent at the end of 2013.[98] If these numbers were to decrease and there was a diversification away from the RMB, this could indicate market predictions that this was not a currency to be handled , hedging against future economic sanctions that could impact these transactions. The signal should be taken even more seriously if we were to see a concentration of this happening with entities based in states considered to be allied to China. This could even suggest some intelligence within these states that a conflict between China and Taiwan was imminent.

Evidence:

1. In a short-term sell-off situation, we could see strong downward pressure on the RMB. The PBOC may intervene to stabilize the currency by selling USD assets.
2. In a longer-term decoupling situation, we would see institutional and other investors introducing policies to stop purchases of RMB-denominated assets, attempts to retrieve their investments in China, and not lending to China.
3. The non-renewal or cancellation of various RMB-denominated trade deals or swap lines.

Recommendations for Policymakers

This section provides four key recommendations to policymakers on how the U.S. can both monitor and influence the development of APMs to leverage its geopolitical interests on the international stage. These recommendations are solely focused on actions the U.S. could take prior to a Chinese invasion of Taiwan, rather than recommendations on post-invasion measures.

Establish an APMs Strategic Coordination Unit

U.S. policymakers should establish an APMs Strategic Coordination Unit to monitor the development of China's APMs strategy, developments that occur in Russia and groupings like BRICS. The unit would be led by officials from the U.S. State Department and report to senior decision-makers at the State Department. The unit would be made up of key stakeholders across government departments, embassies, intelligence agencies, the Commodity Futures Trading Commission and the Securities and Exchange Commission. It would seek input from, and work with, Trump's Working Group on Digital Asset Markets,[99] chaired by new crypto czar David Sacks.[100] The coordination unit would develop its own list of early warning signals, with regular reporting updates on these signals and potential risks to U.S. geopolitical interests. The unit would flex its membership composition depending on the signals being discussed and the levels of confidentiality required.

The six warning signals identified in this policy report, are highlighted in the graphic below.

Early Warning Signals for a Potential Chinese Invasion of Taiwan

1. **BRICS integrates further into other countries***
   Responsible Lead: U.S. State Department
   Composite Members: U.S. Treasury, Central Intelligence Agency
2. **Chinese authorities turn a blind eye to use of non-Know Your Customer digital asset exchanges**
   Responsible Lead: Office of Foreign Assets Control
   Composite Members: U.S. State Department, U.S. Department of Justice, Office of Terrorist Financing and Financial Crimes, U.S. Securities and Exchange Commission, the working group on digital asset markets, blockchain analytics firms **
3. **The Financial Action Task Force (FATF) downgrades China**
   Responsible Lead: Office of Terrorist Financing and Financial Crimes
   Composite Members: U.S. State Department, Office of Foreign Assets Control, U.S. Treasury
4. **China removes legislative restrictions to crypto training in its territories**
   Responsible Lead: U.S. State Department
   Composite Members: U.S. Treasury, Securities and Exchange Commission, the working group on digital asset markets
5. **PBOC purchasing of gold and other non-flat currencies reaccelerates**
   Responsible Lead: U.S. Treasury
   Composite Members: U.S. Federal Reserve, U.S. State Department, Commodity Futures Trading Commission, Securities and Exchange Commission
6. **A growing number of entities that normally trade in RMB pre-emptively switching to other currencies**
   Responsible Lead: U.S. State Department
   Composite Members: U.S. State Department, U.S. Treasury, Commodity Futures Trading Commission, Securities and Exchange Commission

* This should be broken down into smaller individual signals under the BRICS umbrella e.g. the implementation of BCBPI.
** Pending sensitivity of the discussions, external stakeholders, like blockchain analytics firms in this case, could be invited to participate in the coordination unit.

Source: Gavin Moore

The unit's remit would ensure information-gathering and rigorous scrutiny of these signals and serve as a convening body for departments, advisory councils and agencies across government to facilitate a unified, coordinated, and prepared U.S. response to developments in APMs.

Monitor Global CBDC Developments

While it would be for the coordination unit to determine its priority early warning signals, policymakers should closely monitor CBDCs. Trump's "Agenda 47" policy platform explicitly opposed the creation of a U.S. CBDC,[101] with the president also issuing an executive order to prohibit a CBDC being established.[102]

While political appetite for a U.S. CBDC is low, the U.S. must remain vigilant to China's plans for e-CNY on mBridge and potentially a BRICS Bridge. Any contribution China's CBDC could make in reducing other countries' reliance on the USD, and therefore nullify potential future sanctions, will need to be guarded against. Monitoring would also include developments elsewhere, for example a possible European Union CBDC,[103] and how this may impact U.S. interests. Policymakers also should consider alternatives to a CBDC that may achieve similar outcomes. For example, the U.S. could advocate for further reforms to SWIFT, such as the quicker settlement of transactions, to help maintain its position of dominance and confer some of the advantages a U.S. CBDC could offer.

Explore Stablecoins as a Means of Maintaining USD Hegemony

Another area policymakers and the coordination unit will want to pay attention to is the growth of stablecoins , a type of cryptocurrency that aims to maintain a stable value over time, usually by pegging its value to a currency or commodity. The largest stablecoins by market capitalization are currently Tether (USDT) and Circle's (USDC) offerings, which both peg to the USD.[104] Tether itself may have a key ally in the Trump administration: Secretary of Commerce Howard Lutnick, has now stood down from a financial services firm he ran that is the main custodian for Tether's U.S. Treasury bills.[105]

There is bipartisan support for measures that create a more stable regulatory environment for stablecoins in the U.S., such as the introduction of The Guiding and Establishing National Innovation for U.S. Stablecoins, or GENIUS Act.[106] Bank of America CEO Brian Moynihan has also indicated the bank will launch a USD-pegged stablecoin if relevant legislation is passed.[107]

Policymakers may want to consider how a more hospitable regulatory environment in the U.S. could increase the use of USD-backed stablecoins elsewhere. The growth in stablecoin usage outside the U.S. reflects a broader trend in which international markets,[108] which faced with currency volatility, are turning to USD-denominated stablecoins to preserve value and facilitate faster, cheaper transactions.[109]

There has been some pushback. In Europe, the market cap of USDT itself fell as several European exchanges delisted USDT in response to the EU's Markets in Crypto-Assets Regulation entering into force on January 2025.[110] Tether had earlier discontinued support for its euro-pegged stablecoin (EURt) in response to this Regulation.[111,112] Nonetheless, some commentators suggest that stablecoins will be a key factor in USD's continued dominance[113] and should be viewed as a proxy for the dollar's strength as the world's reserve currency. Their performance globally should be monitored closely by the coordination unit, with a particular focus on BRICS members.

Leverage the Deterrent Effect of Sanctions

That sanctions have been effective in weakening Russian GDP[114] or the value of the ruble[115] at all is due to the dominance of USD in the international financial system. Although this has not deterred Russia from persisting with its war in Ukraine,[116] the economic impact of sanctions will help deteriorate its longer-term warfighting capacities. It is paradoxical that the strength of USD in underwriting the effectiveness of these sanctions could ultimately lead to a weakening of USD. The more effective sanctions are, the more they encourage moves away from the dollar by Russia and China to try to blunt their effectiveness. This tension was recognized by former U.S. Treasury Secretary Janet Yellen during testimony to the House Finance Services Committee in July 2024.[117]

How then should policymakers ensure that possible future sanctions remain effective without undermining the USD's position? One way out of this apparent paradox is to recognize the different role sanctions could play in a possible China-Taiwan confrontation. The unprecedented sanctions imposed on Russia since February 2022 have been reactive measures in response to conflict. In the China-Taiwan context, the U.S. should leverage the threat of similar sanctions as a deterrent before conflict has occurred.

This approach would be two-pronged. First, the U.S. could threaten to impose sanctions on China itself. Earlier sections have explored the extent to which China continues to rely on the USD (e.g., its main foreign currency reserve holding) and Western institutions (e.g., CIPS' ongoing reliance on the SWIFT system). China recognizes the impact sanctions could have on its sluggish economy. Chinese banks have been reluctant to do business with sanctioned Russian entities because of the executive orders issued by the Biden administration and determinations from the Office of Foreign Assets Control.[118] Sanctions have clearly had an impact on behavior.

Second, the U.S. should exert diplomatic pressure on countries increasingly under China's influence. This would involve leveraging the threat of secondary sanctions[119] on countries trading with China, were China to invade Taiwan. Or it could involve punitive tariffs for countries thinking about de-dollarization. Trump has already imposed tariffs on China directly in relation to alleged drug trafficking,[120] and has also threatened the use of this policy lever in relation to de-dollarization, stating that if "you leave the dollar, you're not doing business with the United States because we're going to put 100% tariffs on your goods." [121] In either scenario, not only would China suffer from direct sanctions and tariffs but partner countries would also be incentivized to weaken ties, inflicting a further blow to China's APMs strategy.

As noted previously, other members of BRICS have different motivations with respect to China and Russia, such as the ability to easily trade in their local currencies rather than evade sanctions. The U.S. State Department should, through its network of embassies, seek to apply diplomatic pressure, particularly on BRICS-aligned but less enthusiastic supporters of China-Russia led initiative s. Policymakers will therefore want to consider diplomatic levers to isolate China economically from these partners prior to an invasion of Taiwan.

The U.S. may also exert influence over its allies to implement more coordinated sanctions measures. Western governments' secondary sanctions approach on Russia became more aligned at the end of the Biden administration. The U.K. has recently introduced legislative amendments to its sanctions regime, which are thought to create the possibility of secondary sanctions for the first time.[122] The EU has been more reluctant but is reportedly considering moves in the direction of secondary sanctions.[123] [124] Notwithstanding the possibility of the U.S. lifting sanctions on Russia as part of a deal to end the war in Ukraine,[125] the benefits of a coordinated approach would be to increase the deterrent effect of sanctions on China and its economic partners as more jurisdictions implement similar measures to the U.S.

Conclusion

Policymakers should pay greater attention to China's role in the development of APMs, as these provide insight into its intentions for a China-Taiwan conflict. Wars are now fought on many complex and interconnected fronts. Analyzing a specific subsector of conflict, however indirect, can be an illuminating indicator for when a potential conflict becomes a real conflict.

APMs are not the only factor that would indicate an invasion is more likely. However, economic sanctions are now one of the most important levers in warfare shy of direct military involvement. Signals that the potential targets of these sanctions are attempting to reduce their potency – in advance of confrontation – should be taken seriously.

Russia's invasion of Ukraine could mark a turning point in the development of the APMs landscape. The unprecedented Western sanctions that followed may have the paradoxical impact of undermining the USD hegemony on which their effectiveness relies. There has been a noticeable change in Russia's approach to APMs since the invasion to a strategy that is more clearly targeted at blunting the effectiveness of present

and future sanctions. Policymakers will want to closely monitor developments at BRICS, driven by Moscow, as a potentially credible alternative to the Bretton Woods institutions.

There are several signs that China is beginning to shift its approach to APM strategy, U.S. policymakers must assess the implications for two critical areas: (a) maintaining the USD's status as the global reserve currency, and (b) maintaining the effectiveness of sanctions as a foreign policy tool, particularly in the context of an invasion of Taiwan. The four recommendations outlined seek to address to these challenges. These recommendations will ensure that the U.S. is fully prepared to for any APMs developments that indicate an increased likelihood of a China-Taiwan confrontation.

Gavin Moore is a global finance specialist and Director at ForgeFront, a policy and futures consultancy. He has developed cryptocurrency anti-money laundering and terrorist financing rules for a financial regulator and led tariff policy for the UK's Treasury. He has been a head budgetary adviser in the European Parliament and has published works in academic journals and industry outlets.

Endnotes

1 Dress, B. (2024, March 21). China will be ready for potential Taiwan invasion by 2027, US admiral warns. The Hill. https://thehill.com/policy/defense/4547637-china-potential-taiwan-invasion-2027-us-admiral-warns/

See also the subsequent report, the Commission on the National Defense Strategy: https://www.armed-services.senate.gov/imo/media/doc/nds_commission_final_report.pd

2 Harman, J., Edelman, E., Mahnken, T. G., Sixkiller, M., Starzak, A., & Zakheim, R. (2024). Report of the Commission on the National Defense Strategy. RAND. https://www.armed-services.senate.gov/imo/media/doc/nds_commission_final_report.pdf

3 GJ Open. (2025, February 27). Will there be a lethal confrontation between the national military forces, militia, and/or law enforcement personnel (Forces) of Taiwan and the People's Republic of China (PRC) before 1 October 2025?. https://www.gjopen.com/questions/3747-will-there-be-a-lethal-confrontation-between-the-national-military-forces-militia-and-or-law-enforcement-personnel-forces-of-taiwan-and-those-of-the-people-s-republic-of-china-prc-before-1-october-2025/crowd_forecast

4 China is using an "anaconda strategy" to squeeze Taiwan. (2024, October 3). The Economist. https://www.economist.com/asia/2024/10/03/china-is-using-an-anaconda-strategy-to-squeeze-taiwan

5 U.K. Ministry of Foreign Affairs. (2022, October 4). What is the impact of the war in Ukraine on exports of vegetable oils?. https://www.cbi.eu/market-information/grains-pulses-oilseeds/what-impact-war-ukraine-exports-vegetable-oils.

6 Shahbandeh, M. (2024, February 28). Export volume of sunflowerseed oil worldwide from 2016/17 to 2023/24, by country (in 1,000 metric tons). Statista. https://www.statista.com/statistics/620317/sunflowerseed-oil-export-volume-worldwide-by-country/

7 Winston, K. (2024, September 4). Recent Houthi attacks suggest new focus on oil tankers: Yemen-based expert. S&P Global. https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/oil/090424-recent-houthi-attacks-suggest-new-focus-on-oil-tankers-yemen-based-expert

8 A central bank digital currency (CBDC) is a form of digital currency issued by a country's central bank. It is similar to cryptocurrencies, except that its value is fixed by the central bank and is equivalent to the country's fiat currency i.e. the USD or the British Pound. As a digital liability of a central bank, CBDCs are thought to be less volatile than other cryptocurrencies.

9 Federal Reserve Bank of St. Louis. (2024, November 25). Total Reserves excluding Gold for China. https://fred.stlouisfed.org/series/TRESEGCNM052N

10 The currency of the People's Republic of China is referred to interchangeably as either the Chinese yuan (CNY) or renminbi (RMB). The key difference is that the RMB is the official currency, while the yuan is its principal unit of measurement. The equivalent in U.S. terms would be for RMB read U.S. Dollar, and for yuan read dollar.

11 BBC. (2012, May 8). China buying oil from Iran with Yuan. https://www.bbc.co.uk/news/business-17988142

12 Chang, C., Rana, V., Gupta, Z., & Rezvijs, V. (2024, August 20). Saudi-China ties and renminbi-based oil trade. S&P Global. https://www.spglobal.com/en/research-insights/special-reports/saudi-china-ties-and-renminbi-based-oil-trade

13 Here, we use J.P.Morgan's definition of de-dollarization, which "entails a significant reduction in the use of dollars in world trade and financial transactions, decreasing national, institutional and corporate demand for the greenback. This would diminish the dominance of the dollar-denominated global capital markets, in which borrowers and lenders around the world transact in dollars." https://www.jpmorgan.com/insights/global-research/currencies/de-dollarization
J. P. Morgan. (2024, October 8). De-dollarization: Is the US dollar losing its dominance?. https://www.jpmorgan.com/insights/global-research/currencies/de-dollarization

14 The Trump Administration may deem current reserve rates as a baseline from which to measure success of this policy. IMF data show's 58.22 percent of allocated reserves were held in USD in Q2 2024, with 19.76 percent in Euro as the closest challenger and only 2.14 percent in RMB. https://data.imf.org/?sk=e6a5f467-c14b-4aa8-9f6d-5a09ec4e62a4

15 Republican Party. (2024, July 8). 2024 GOP Platform Make America Great Again!, 9. https://prod-static.gop.com/media/RNC2024-Platform.pdf?_gl=1*1kwqi4o*_gcl_au*MjMzMjk5Mzc5LjE3MzMzNjQ1ODI.&_ga=2.79801364.2029520348.1734397581-53960822.1733364582

16 At the time of writing (Feb. 27, 2025), 18,381 designations have been made. The seven jurisdictions covered in the Atlantic Council's database are the U.S., the U.K., the European Union, Switzerland, Canada, Australia, and Japan: https://www.atlanticcouncil.org/blogs/econographics/russia-sanctions-database/

Atlantic Council. (2024). Russia Sanctions Database. https://www.atlanticcouncil.org/blogs/econographics/russia-sanctions-database/

17 Exec. Order No. 14,114, 3 C.F.R. 89271-89274 (2023). https://www.federalregister.gov/documents/2023/12/26/2023-28662/taking-additional-steps-with-respect-to-the-russian-federations-harmful-activities

18 Dual-use items (including software and technology) are items which can be used for both civil and military purposes. The term also includes all goods which have non-explosive uses or assist in any way with the manufacture of nuclear weapons or other nuclear explosive devices. https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources

U.K. Export Control Joint Unit. (2019, September 24). Export controls: dual-use items, software and technology, goods for torture and radioactive services. https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources

19 Gan., N. (2024, October 18). US imposes first sanctions on Chinese firms for making weapons for Russia's war in Ukraine. CNN. https://edition.cnn.com/2024/10/18/china/us-sanctions-chinese-companies-attack-drones-russia-intl-hnk/index.html

20 Liu, Z. Z., & Papa, M. (2022). Can BRICS De-dollarize the Global Financial System? Cambridge: Cambridge University Press.

21 Todorova, V., Moraliyska, M. & Raycheva, I. (2024). De-Dollarisation in International Payments: Trend or Fiction. ECONOMICS, 12(2), 129-144. https://doi.org/10.2478/eoik-2024-0018

22 Shah, M. U., Gill, Q. S., Akhtar, M. N., & Mustafa, G. (2024). Understanding the Decline of the US Dollar: Key Factors and Implications. Journal of Social &Amp; Organizational Matters, 3(2), 234–250. https://doi.org/10.56976/jsom.v3i2.81

23 Silk, L. (1973, July 4). The Dollar's Tribulations. The New York Times. https://www.nytimes.com/1973/07/04/archives/the-dollars-tribulations-currency-remains-essentially-strong-but-it.html

24 China's yuan is nowhere close to displacing the greenback. (2024, October 14). The Economist. https://www.economist.com/special-report/2024/10/14/chinas-yuan-is-nowhere-close-to-displacing-the-greenback

25 Gopinath, G. (2024, May 7). Geopolitics and its Impact on Global Trade and the Dollar. International Monetary Fund. https://www.imf.org/en/News/Articles/2024/05/07/sp-geopolitics-impact-global-trade-and-dollar-gita-gopinath

26 Pismennaya, E., & Biryukov, A. (2022, January 20). Bank of Russia Seeks to Outlaw Crypto Mining, Trading. Bloomberg. https://www.bloomberg.com/news/articles/2022-01-20/russia-s-fsb-tells-nabiullina-to-ban-crypto-to-defund-opposition?embedded-checkout=true

27 Artemchuk, O. (2024, September 17). Russia pays China in cryptocurrency for goods it needs for war. Ukrainska Pravda. https://www.pravda.com.ua/eng/news/2024/09/17/7475467/

28 Feingold, S. (2023, March 16). Why the role of crypto is huge in the Ukraine war. World Economic Forum. https://www.weforum.org/stories/2023/03/the-role-cryptocurrency-crypto-huge-in-ukraine-war-russia/

29 Blockchain analytics firm Elliptic noted that pro-Ukrainian fundraisers had raised over $212 million in cryptoassets since the beginning of the war in February 2022 until March 2023. This has substantially outpaced pro-Russian crypto donations, which stand at $4.8 million. A further $0.7 million has been raised by anti-government entities in Belarus, which is a key ally of Russia https://www.elliptic.co/blog/analysis/crypto-donations-to-ukraine-and-russia-breaking-down-the-numbers

Elliptic. (2023, March 3). Crypto donations to Ukraine and Russia: breaking down the numbers. https://www.elliptic.co/blog/analysis/crypto-donations-to-ukraine-and-russia-breaking-down-the-numbers

30 Chainalysis. (2024, September 5). Russia's Cryptocurrency Pivot: Legislated Sanctions Evasion. https://www.chainalysis.com/blog/russias-cryptocurrency-legislated-sanctions-evasion/

31 Napolitano, L. (2024, December 15). Bitcoin Is Flying High – These Countries are Considering a National Reserve. decrypt. https://decrypt.co/294154/bitcoin-national-reserve-countries

32 Ledger Insights. (2024, November 28). Retailers push for a delay in rollouts of Russia's CBDC. https://www.ledgerinsights.com/retailers-push-for-a-delay-in-rollout-of-russias-cbdc/

33 Digital Pound Foundation. (2024, October 3). Russia Adjusts Digital Rouble Rollout, Mandating CBDC Acceptance by July 2025. https://digitalpoundfoundation.com/russia-adjusts-digital-rouble-rollout-mandating-cbdc-acceptance-by-july-2025/

34 Hawser, A. (2024, September 6). Push for alternatives to US dollar and new payment systems accelerates as sanctions scale. The Banker. https://www.thebanker.com/Push-for-alternatives-to-US-dollar-and-new-payment-systems-accelerates-as-sanctions-scale-1725622890

35 Kremlin. (2024, July 17). Economic Affairs Meeting. Kremlin. http://kremlin.ru/events/president/news/74566

36 Hotten, R. (2022, May 4). Ukraine conflict: What is Swift and why is banning Russia so significant?. BBC. https://www.bbc.co.uk/news/business-60521822

37 Richter, F. (2024, October 22). U.S. Dollar Dominates Global Payment Network SWIFT. statista. https://www.statista.com/chart/26943/currency-composition-of-payments-processed-on-swift/

38 G7, EU to target banks with sanctions using Russia's SPFS money transfer system. (2024, June 3). Intellinews. https://www.intellinews.com/g7-eu-to-target-banks-with-sanctions-using-russia-s-spfs-money-transfer-system-328031/

39 Interfax. (2024, June 26). Solution will be found for latest EU sanctions against financial messaging system; will continue operating in 'proper mode' – Russian Central Bank. https://interfax.com/newsroom/top-stories/103743/

40 Council of the European Union. (2024, December 16). EU sanctions against Russia explained. https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/

41 Curtis, J. (2024). The BRICS group: Overview and recent expansion. U.K. Parliament. https://commonslibrary.parliament.uk/research-briefings/cbp-10136/

42 Note: this figure includes Saudi Arabia which has been invited to join BRICS but is yet to formally accept. Argentina was also invited but has declined membership. Afota, A., Burban, V., Diev, P., Grieco, F., Iberrakene, T., Ishii, K., Lopez-Forero, M., Paul, Q., Sammeth, F., & Valadier, C. (2024, February 13). Expansion of BRICS: what are the potential consequences for the global economy? Banque de France. https://www.banque-france.fr/en/publications-and-statistics/publications/expansion-brics-what-are-potential-consequences-global-economy

43 Monin, S. (2024, October 24). BRICS approves Cuba, Bolivia, and 11 other countries as 'partner states.' Brasil de Fato. https://www.brasildefato.com.br/2024/10/24/brics-approves-cuba-bolivia-and-11-other-countries-as-partner-states

44 BRICS. (2024, October 23). Kazan Declaration: Strengthening multilateralism for just global development and security. https://cdn.brics-russia2024.ru/upload/docs/Kazan_Declaration_FINAL.pdf?1729693488349783

45 Everington, J., & Hawser, A. (2024, October 25). Explainer: Putin's Swift rival a bridge too far for Brics. The Banker. https://www.thebanker.com/Explainer-Putin-s-Swift-rival-a-bridge-too-far-for-Brics-1729858688

46 Putin's plan to dethrone the dollar. (2024, October 20). The Economist. https://www.economist.com/international/2024/10/20/putins-plan-to-dethrone-the-dollar

47 Putin, V. (2024, October 24). News Conference Following 16th BRICS Summit. BRICS-Russia 2024. https://brics-russia2024.ru/en/news/press-konferentsiya-po-itogam-xvi-sammita-briks/

48 Everington, J., & Hawser, A. (2024, October 25). Explainer: Putin's Swift rival a bridge too far for Brics. The Banker. https://www.thebanker.com/Explainer-Putin-s-Swift-rival-a-bridge-too-far-for-Brics-1729858688

49 BRICS payment system would not replace SWIFT – S.Africa finance minister. (2023, August 24). Reuters. https://www.reuters.com/world/africa/brics-payment-system-would-not-replace-swift-safrica-finance-minister-2023-08-24/

50 Lawder, D., & Rajan, G. (2025, February 21). US Treasury's Bessent says Russia could win sanctions relief in war talks. Reuters. https://www.reuters.com/world/us-treasurys-bessent-says-russia-could-win-sanctions-relief-war-talks-2025-02-20/

51 Gopinath, G. (2024, May 7). Geopolitics and its Impact on Global Trade and the Dollar. The International Monetary Fund. https://www.imf.org/en/News/Articles/2024/05/07/sp-geopolitics-impact-global-trade-and-dollar-gita-gopinath

52 Gopinath, G. (2024, May 7). Geopolitics and its Impact on Global Trade and the Dollar. The International Monetary Fund. https://www.imf.org/en/News/Articles/2024/05/07/sp-geopolitics-impact-global-trade-and-dollar-gita-gopinath

53 Richter, F. (2024, October 22). U.S. Dollar Dominates Global Payment Network SWIFT. statista. https://www.statista.com/chart/26943/currency-composition-of-payments-processed-on-swift/

54 Greene, R. (2023, December 5). The Difficult Realities of the BRICS' Dedollarization Efforts – the Renminbi's Role. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/12/the-difficult-realities-of-the-brics-dedollarization-effortsand-the-renminbis-role?lang=en

55 Yeung, R., & Goh, K. 2022. Petroyuan Will Not Bring About a Regime Shift Soon. ANZ Research, China Insight.

56 Greene, R. (2023, December 5). The Difficult Realities of the BRICS' Dedollarization Efforts – and the Renminbi's Role. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/12/the-difficult-realities-of-the-brics-dedollarization-effortsand-the-renminbis-role?lang=en

57 Hennessy, L. (2024, August 16). Digital Yuan: A Global Game-Changer in the Era of Central Bank Digital Currencies (CBDCs). Clyde & Co. https://www.clydeco.com/en/insights/2024/09/digital-yuan-a-global-game-changer-in-the-era-of-c

58 Digital Pound Foundation. (2024, October 12). China Reports Rapid Growth for Digital Yuan: 180 Million Wallets and 7 Trillion Yuan in CBDC Transactions. https://digitalpoundfoundation.com/china-reports-rapid-growth-for-digital-yuan-180-million-wallets-and-7-trillion-yuan-in-cbdc-transactions/

59 Ledger Insights. (2023, March 7). Digital yuan enabled WeChat Pay. More Hong Kong e-CNY trials. https://www.ledgerinsights.com/digital-yuan-wechat-hong-kong-e-cny-cbdc/

60 BIS Innovation Hub. (2022). Project mBridge: Connecting economies through CBDC. Bank for International Settlements. https://www.bis.org/publ/othp59.pdf

61 Bank for International Settlements. (2024, November 11). Project mBridge reached minimum viable product stage. https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm

62 Davier, M. (2024, January 30). UAE Completes First Cross-Border Digital Dirham CBDC Payment Worth $13.6M to China. yahoo!finance. https://finance.yahoo.com/news/uae-completes-first-cross-border-121427265.html

63 China declares all crypto-currency transactions illegal. (2021, September 24). BBC. https://www.bbc.co.uk/news/technology-58678907

64 Shen, X. (2024, December 31). China's new forex rules require banks to tighten scrutiny on cryptocurrency trades. South China Morning Post. https://www.scmp.com/tech/blockchain/article/3292795/chinas-new-forex-rules-require-banks-tighten-scrutiny-cryptocurrency-trades

65 Parker, E. (2024, February 5). China Never Completely Banned Crypto. Nasdaq. https://www.nasdaq.com/articles/china-never-completely-banned-crypto

66 China declares all crypto-currency transactions illegal. (2021, September 24). BBC. https://www.bbc.co.uk/news/technology-58678907

67 Shin, F. (2022, January 31). What's behind China's cryptocurrency ban?. World Economic Forum. https://www.weforum.org/stories/2022/01/what-s-behind-china-s-cryptocurrency-ban/

68 Reguerra, E. (2025, January 1). China tightens crypto trade oversight with new forex rules. Coin Telegraph. https://cointelegraph.com/news/china-banks-crypto-transaction-scrutiny

69 Chainalysis. (2024, September 17). Eastern Asia: Institutions Drive Adoption in South Korea and Hong Kong. https://www.chainalysis.com/blog/eastern-asia-crypto-adoption-2024/

70 China's yuan is nowhere close to displacing the greenback. (2024, October 14). The Economist. https://www.economist.com/special-report/2024/10/14/chinas-yuan-is-nowhere-close-to-displacing-the-greenback

71 China's Xi criticizes sanctions at meeting of BRICS nations. (2022, June 23). AP News. https://apnews.com/article/russia-ukraine-putin-jair-bolsonaro-beijing-d13c56ed449bd2570fe224bc316d6d24

72 World Gold Council. (2024, December 4). Gold Reserves by Country. https://www.gold.org/goldhub/data/gold-reserves-by-country

73 Moss, J. (2024, August 14). What's behind China's gold-buying spree?. International Banker. https://internationalbanker.com/banking/whats-behind-chinas-gold-buying-spree/

74 Gopinath, G. (2024, May 7). Geopolitics and its Impact on Global Trade and the Dollar. The International Monetary Fund. https://www.imf.org/en/News/Articles/2024/05/07/sp-geopolitics-impact-global-trade-and-dollar-gita-gopinath

75 Gopinath, G. (2024, May 7). Geopolitics and its Impact on Global Trade and the Dollar. The International Monetary Fund. https://www.imf.org/en/News/Articles/2024/05/07/sp-geopolitics-impact-global-trade-and-dollar-gita-gopinath

76 Lawford, M. (2024, April 30). China's $170bn gold rush triggers Taiwan invasion fears. The Telegraph. https://www.telegraph.co.uk/business/2024/04/30/china-launches-gold-buying-spree-amid-fears-o/

77 Atkinsons. (2023). An Interactive Map: The world's largest gold reserves. https://atkinsonsbullion.com/gold/worlds-largest-gold-reserves-map

78 Jia, R. (2025, February 18). China's gold market update: Central bank purchases continue in January. World Gold Council. https://www.gold.org/goldhub/gold-focus/2025/02/chinas-gold-market-update-central-bank-purchases-continue-january

79 Everington, J., & Hawser, A. (2024, October 25). Explainer: Putin's Swift rival a bridge too far for Brics. The Banker. https://www.thebanker.com/Explainer-Putin-s-Swift-rival-a-bridge-too-far-for-Brics-1729858688

80 Project mBridge unsettled by geopolitical jockeying. (2024, October 31). DigFin. https://www.digfingroup.com/mbridge-bis/

81 Putin's plan to dethrone the dollar. (2024, October 20). The Economist. https://www.economist.com/international/2024/10/20/putins-plan-to-dethrone-the-dollar

82 Long, K. (2024, October 31). Explainer: BIS backs out of CBDC project mBridge. The Banker. https://www.thebanker.com/Explainer-BIS-backs-out-of-CBDC-project-mBridge-1730397119

83 Madureira, V. (2022, October 3). China Arrests 93 Members of a Criminal Group Over Alleged $5.6B Crypto Fraud. Organized Crime and Corruption Reporting Project. https://www.occrp.org/en/news/china-arrests-93-members-of-a-criminal-group-over-alleged-56b-crypto-fraud

84 Chainalysis. (2024, September 4). Russia's Cryptocurrency Pivot: Legislated Sanctions Evasion. https://www.chainalysis.com/blog/russias-cryptocurrency-legislated-sanctions-evasion/

85 Chainalysis. (2024, August 29). 2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks On The Rise, Pig Butchering Scams Remain Lucrative. https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/

86 Financial Action Task Force. (2019). Anti-money laundering and counter-terrorist financing measures – People's Republic of China. https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-china-2019.html

87 Huang, R. (2024, July 24). Will China Unban Bitcoin, Creating a Huge Bitcoin Price Bump?. Forbes. https://www.forbes.com/sites/digital-assets/2024/07/24/will-china-unban-bitcoin-creating-a-huge-bitcoin-price-bump/

88 Katte, S. (2024, August 20). China supreme court revises Anti-Money Laundering law to include 'virtual assets.' Cointelegraph. https://cointelegraph.com/news/china-revises-anti-money-laundering-law-include-crypto

89 A series of Trump hires are perceived to signal a move to a more lenient regulatory environment for cryptocurrencies, including nominating Paul Atkins as the new chair of the Securities and Exchange Commission, with Mark Uyeda as acting chair; Brian Quintenz as the new chair of the Commodity Futures Trading Commission, with Caroline Pham as acting chair. Trump's 2024 co-campaign manager Chris LaCivita has joined Coinbase, a cryptocurrency exchange platform's Global Advisory Council.

Qureshi, M. (2025, January 16). Trump reportedly 'receptive' to strategic reserve with US-based cryptos. Cointelegraph. https://cointelegraph.com/news/trump-receptive-strategic-reserve-us-cryptos

Ligon, C. (2025, January 21). SEC Forms New Crypto Task Force Spearheaded by Hester Peirce. Coindesk. https://www.coindesk.com/policy/2025/01/21/sec-forms-new-crypto-task-force-spearheaded-by-hester-peirc

Nikhilesh, D., & Hamilton, J. (2025, February 12). Trump to Tap Former CFTC Commissioner, a16z Policy Head Brian Quintenz for CFTC Head. Coindesk. https://www.coindesk.com/policy/2025/02/11/trump-taps-former-cftc-commissioner-a16z-policy-head-brian-quintenz-for-cftc-head

Khatri, Y. (2025, February 14). Coinbase adds Trump campaign manager, ex-Senator and two others to advisory council. Coinbase. https://www.theblock.co/post/337664/coinbase-global-advisory-council-hires

90 China Considers Lifting its Crypto Ban as Trump Wins Presidential Elections – Could this New Layer-2 Project Ride The Potential Bull Wave?. (2024, November 18). Techpointafrica. https://techpoint.africa/2024/11/18/china-considers-lifting-its-crypto-ban-as-trump-wins-presidential-elections-could-this-new-layer-2-project-ride-the-potential-bull-wave/

91 Cooling, S. (2024, December 10). China Likely to Build Bitcoin Reserve After U.S. Sets Precedent, Says Binance's CZ. Cryptonews. https://cryptonews.com/news/china-likely-to-build-bitcoin-reserve-after-u-s-sets-precedent-says-binance-cz/

92 McGleenon, B. (2024, February 4). Trump's 'crypto czar' floats bitcoin reserve as White House pushes sovereign wealth fund. The Block. https://www.theblock.co/post/338761/bitcoin-could-be-part-of-us-sovereign-wealth-fund-plan-says-trumps-crypto-czar

93 Watson, RT. (2024, December 12). Trump remains keen on strategic crypto reserve with aim of making US industry leader. The Block. https://www.theblock.co/post/330616/trump-remains-keen-on-strategic-crypto-reserve-with-aim-of-making-us-industry-leader

94 Chainalysis. (2024, September 17). Eastern Asia: Institutions Drive Adoption in South Korea and Hong Kong. https://www.chainalysis.com/blog/eastern-asia-crypto-adoption-2024/

95 Ho-him, C., & Wiggins, K. (2024, November 28). Hong Kong plans crypto tax break for hedge funds and billionare families. Financial Times. https://www.ft.com/content/543829f0-c07a-43ed-a3e4-57759ca79285

96 Chaddah, M. (2023, June 1). Hong Kong to be digital asset rules sandbox for China, says former city regulator. Forkast. https://forkast.news/hong-kong-crypto-regulatory-sandbox-for-china/

97 Jia, R. (2025, February 18). China's gold market update: Central bank purchases continue in January. World Gold Council. https://www.gold.org/goldhub/gold-focus/2025/02/chinas-gold-market-update-central-bank-purchases-continue-january

98 Goldman Sachs. (2023, July 26). China's currency rises in cross-border trade but remains limited globally. https://www.goldmansachs.com/insights/articles/chinas-currency-rises-in-cross-border-trade-but-remains-limited-globally

99 The White House. (2025, January 23). Strengthening American Leadership in Digital Financial Technology. https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/

100 Trump appoints former PayPal exec David Sacks as AI and crypto czar. (2024, December 6). Reuters. https://www.reuters.com/world/us/trump-appoints-former-paypal-coo-david-sacks-ai-crypto-czar-2024-12-06/

101 Republican Party. (2024, July 8). 2024 GOP Platform Make America Great Again!, 9. https://prod-static.gop.com/media/RNC2024-Platform.pdf?_gl=1*1kwqi4o*_gcl_au*MjMzMjk5Mzc5LjE3MzMzNjQ1ODI.&_ga=2.79801364.2029520348.1734397581-53960822.1733364582

102 The White House. (2025, January 23). Strengthening American Leadership in Digital Financial Technology. https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/

103 McGleenon, B. (2024, December 2). ECB advances digital euro project with new progress report. The Block. https://www.theblock.co/post/328994/ecb-advances-digital-euro-project-with-new-progress-report

104 CoinMarketCap. (n.d.). Top Stablecoins by Market Capitalization. Retrieved December 16, 2024, from https://coinmarketcap.com/view/stablecoin/

105 Schwartz, L. (2024, November 25). Tether was an outlaw for years. Now the $132 billion stablecoin has a key ally in Trump's cabinet. Fortune. https://fortune.com/crypto/2024/11/25/commerce-nominee-howard-lutnick-tether-booster-cantor-fitzgerald/

106 Wynn, S. (2025, February 26). Sen. Lummis says Washington is 'on the precipice' of stablecoin and crypto regulation bills. The Block. https://www.theblock.co/post/343638/sen-lummis-says-washington-is-on-the-precipice-of-stablecoin-and-crypto-regulation-bills

107 Ramos, J. (2025, February 26). Bank of America to Launch USD-Pegged Crypto Stablecoin. Watcher.Guru. https://watcher.guru/news/bank-of-america-to-launch-usd-pegged-crypto-stablecoin

108 Chainalysis. (2024, October 23). Stablecoins dominate market share, Bitcoin grows, and merchant services thrive in Central, Northern, & Western Europe. https://www.chainalysis.com/blog/2024-western-europe-crypto-adoption/

109 US lagging behind in global stablecoin adoption – Chainalysis. (2024, October 17). FXStreet. https://www.fxstreet.com/cryptocurrencies/news/us-lagging-behind-in-global-stablecoin-adoption-chainalysis-202410170738

110 Jaupi, J. (2025, January 2). Tether's Market Cap Sheds $3 Billion as Europe's MiCA Regulations Take Effect. The Defiant. https://thedefiant.io/news/defi/tether-s-market-cap-sheds-usd3-billion-as-europe-s-mica-regulations-take-effect

111 Partz, H. (2024, November 27). Tether discontinues support for euro-pegged stablecoin EURt. Cointelegraph. https://cointelegraph.com/news/tether-discontinues-euro-eurt-stablecoin

112 Azizov, A. (2024, December 17). Stablecoins will see explosive growth in 2025 as world embraces asset class. Cointelegraph. https://cointelegraph.com/news/stablecoins-will-see-explosive-growth-in-2025-as-world-embraces-asset-class

113 Cowen, T. (2024, October 29). Don't Bet Against the Dollar. Bloomberg. https://www.bloomberg.com/opinion/articles/2024-10-29/don-t-bet-against-the-dollar

114 Lyngaas, R. (2023, December 14). Sanctions and Russia's War: Limiting Putin's Capabilities. U.S. Department of Treasury. https://home.treasury.gov/news/featured-stories/sanctions-and-russias-war-limiting-putins-capabilities

115 Russia's plunging currency spells trouble for its war effort. (2024, December 1). The Economist. https://www.economist.com/finance-and-economics/2024/12/01/russias-plunging-currency-spells-trouble-for-its-war-effort

116 Lister, T. (2024, January 29). Russia boasts it is beating sanctions, but its longer-term prospects are bleak. CNN. https://edition.cnn.com/2024/01/29/europe/russia-sanctions-putin-ukraine-economy-intl/index.html

117 The Annual Testimony of the Secretary of the Treasury on the State of the International Financial System: Hearing before the House Financial Services Committee, 118th Cong. (2024). https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=409309

118 van Brugen, I. (2024, July 5). Putin's Top Banker Issues Somber Warning on Chinese Currency. Newsweek. https://www.newsweek.com/russia-central-bank-yuan-china-sanctions-1921411

119 Dow Jones. (n.d.). What are secondary sanctions?. https://www.dowjones.com/professional/risk/glossary/sanctions/secondary-sanctions/

120 Sherman, N. (2025, February 27). Trump says US will impose additional 10% tariff on China. BBC. https://www.bbc.co.uk/news/articles/ce8yy3wpn6eo

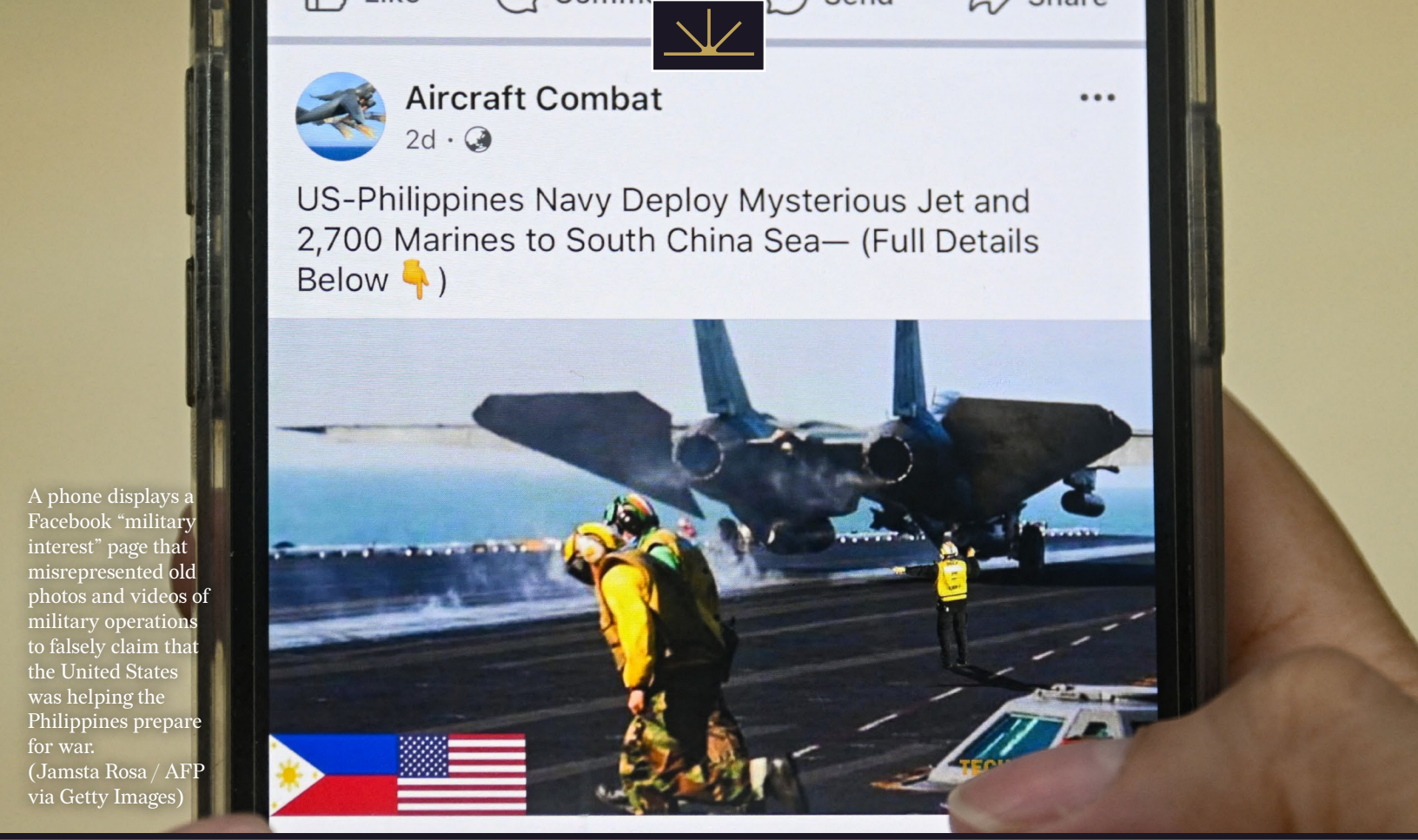
121 Butts, D. (2024, September 9). Trump's vow of 100% tariffs on nations that snub the dollar is a lose-lose for China and the U.S., economist says. CNBC. https://www.cnbc.com/2024/09/09/economist-calls-trumps-threat-to-tariff-countries-that-shun-the-dollar-a-lose-lose.html

122 New UK Sanctions Designation Criteria – A move towards "Secondary Sanctions"?. (2024, August 28). Eversheds Sutherland. https://www.eversheds-sutherland.com/en/global/insights/new-uk-sanctions-designation-criteria

123 Savic, B. (2024, August 12). Risky EU approach to tightening Russia sanctions. GIS Reports Online. https://www.gisreportsonline.com/r/eu-extraterritorial-sanctions-russia/

124 Mahle, M. B. (2024, September 22). Extra-Territorial Sanctions Policies of UK, EU and Canada Creep Closer to the US. Steptoe. https://www.steptoe.com/en/news-publications/stepwise-risk-outlook/stepwise-risk-outlook-deep-dive-extra-territorial-sanctions-policies-of-uk-eu-and-canada-creep-closer-to-the-us.html

125 Lawder, D., & Rajan, G. (2025, February 21). US Treasury's Bessent says Russia could win sanctions relief in war talks. Reuters. https://www.reuters.com/world/us-treasurys-bessent-says-russia-could-win-sanctions-relief-war-talks-2025-02-20/



A phone displays a Facebook "military interest" page that misrepresented old photos and videos of military operations to falsely claim that the United States was helping the Philippines prepare for war. (Jamsta Rosa / AFP via Getty Images)

The Double-Edged Sword: How to Win the War on Fake News

Sam Douglas-Bate

Introduction

Misinformation, defined as false content a publisher believes to be true, and disinformation, defined as false content that a publisher knows to be untrue, pose major threats to U.S. society. Most adults in the U.S. report seeing false or misleading information online at least weekly.[1] Artificial intelligence (AI), augmented and virtual reality, the "internet of things," and wireless technologies are increasingly bringing people together but have also elevated their exposure to fake news, which comprises both misinformation and disinformation. Events such as the riot at the U.S. Capitol on Jan. 6, 2021, may become more common as people are influenced by real and fake social media accounts, bot networks, and troll farms deploying fake news that leads to unrest. However, new technologies are a double-edged sword: They can provide defenses to false and misleading information though technologies such as digital watermarks, AI classifiers, user dashboards, and application programming interfaces (APIs) that make it easier for people to sort what is true from what is false.

In the runup to the 2024 presidential election, a "whirlwind"[2] of fake news around voter fraud emerged on social media platforms. Federal investigators described Russia as the "most active threat"[3] during the period with alleged Kremlin-backed online accounts posting and amplifying articles pushing false election fraud narratives. For example, U.S. intelligence

agencies explained that one widely shared piece of content, which allegedly showed people from the Haitian community illegally voting, was fabricated by "Russian influence actors."[4]

While Russia represents a bigger existing threat, the risk of similar activity from China needs to be taken seriously given geopolitical competition is likely to escalate during the Trump presidency. While the National Intelligence Council (NIC) assessed that Beijing did not attempt to influence the 2020 presidential elections,[5] an increase in the spread of fake news by Chinese-linked actors was seen in 2024. The prospect is more alarming in light of China's online information campaigns. While measuring the levels of fake news originating from sources is fraught with complexity, the country undoubtedly plays host to one the world's most sophisticated influencing operations.

"Spamouflage," also known as "Dragonbridge," is a wide online network of Chinese actors that has sought to promote Beijing's national interests by creating and posting fake news. Microsoft estimates Spamouflage's influence operation targets 175 websites and 58 languages.[6] Meta announced in August 2023 that it had taken down thousands of China-linked Facebook pages and claimed it to be the "largest known cross-platform covert influence operation in the world."[7] U.S. policymakers must act accordingly.

The spread of fake news is a cross-cutting issue that adds fuel to the fire by augmenting three areas prioritized by lawmakers in their interaction with Beijing:[8] competition in the South China Sea, hacking of U.S. infrastructure,[9] and economic competition. Furthermore, any fake news, whether from China or elsewhere, has widespread implications for public trust in government, the electoral process, and much more besides.

The War of Words

Ever since the Chinese Communist Party came to power, China and the U.S. have exchanged terse diplomatic language on issues pertaining to influence over each other's national life. This stands in stark contrast to China's well acknowledged and publicly proclaimed commitment of noninterference in other countries' internal affairs.[10] In many cases, the two have accused each other publicly of spreading fake news. As recently as February 2023, Chinese representatives to the U.N. claimed the U.S. had used biological weapons in North Korea in the 1950s,[11] an accusation the U.S. strongly denies.[12] China has accused the U.S. military of spreading "anti-vax" misinformation during the COVID-19 pandemic, a claim that was backed up by Reuters research.[13] More recently, these claims surfaced again on Chinese social media.[14]

The risk of Chinese-backed actors spreading fake news is increasing. Despite the NIC's assessment of the 2020 vote, research from Microsoft found that Chinese influence campaigns targeted the 2024 elections and were focused on Republican candidates who had known "anti-China" stances. These accounts "parroted antisemitic messages, amplified accusations of corruption, and promoted opposition candidates."[15] Analysis concluded that Spamouflage accounts did not favor one presidential candidate but instead focused on down-ballot elections to sway local results. Influence attempts by Beijing-backed actors included impersonating Americans, spreading inflammatory messaging[16] on cultural issues, and even amplifying Russian interference attempts.[17]

The Impact of Foreign Influence Campaigns

While China has been culpable of spreading fake news in the U.S., Russia is often cited as the main state orchestrator of such campaigns. It is worth noting, too, that recent conspiracy theories, such as that the U.S. government manipulated Hurricane Milton, or relating to the motivations behind the assassination attempt on Donald Trump in Pennsylvania , originated in the U.S. rather than abroad. Domestic technology can also be to blame for false information, with recent research by Full Fact showing that Amazon Alexa, partly built in California and accessible via half a billion devices globally, has supplied users with incorrect information on a number of important topics.[18]

However, because of China's rapidly increasing technological maturity, policymakers need to take a new approach to counter fake news from Beijing-linked actors. Chinese President Xi Jinping has talked openly of using AI in "news collection, production, distribution, reception and feedback,"[19] state-backed media outlets

have talked about its relevance for "construction of international communication capabilities,"[20] and researchers have claimed the Chinese military is "clearly interested"[21] in leveraging AI for social media manipulation.

Chinese fake social media accounts, bot networks, troll farms, and content farms, as well as more traditional state-run media and wolf diplomacy, have been used to push fake news. Chinese actors are increasingly using new technologies including deepfakes and generative AI to create a large amount of new content quickly.[22]

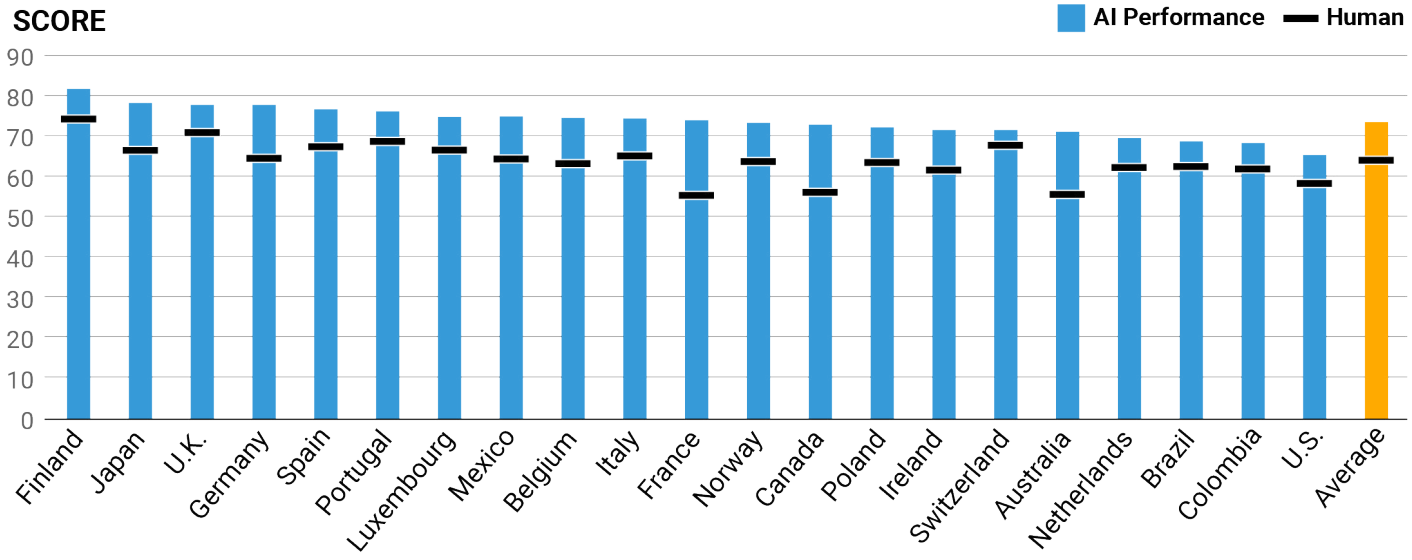
Tackling the growing issue requires balancing freedoms, such as the First Amendment, with penalties for foreign actors spreading fake news. Domestic approaches to combating the issue could include establishing incentives for the private sector to provide new ways of delivering impartial fact-checking and, as seen with the use of X's established and Meta's new Community Notes programs, encouraging the public to have the agency to do their own research. Any government approach should be consistent regardless of the source of the fake news, whether foreign or domestic.

Beijing's influence campaigns have not improved China's image among U.S. citizens. In the last five years, Americans claiming to have an unfavorable view of the country has grown from 47% to 81%.[23] However, fake news campaigns are complex, and reversing such a trend may not be the primary goal of Chinese actors.

A survey by the Organization for Economic Cooperation and Development (OECD) of citizens in 21 countries shows that U.S. users rank last in their ability to identify AI generated disinformation and third-to-last in their capability to recognize human generated disinformation (see Graphic 1).[24] The AI statistic is particularly alarming when considering the ease with which malign actors can now quickly create large influence campaigns in any language online. There is a distinct likelihood that these campaigns will become more sophisticated and believable in the future as technologies, such as deepfakes, improve.

A large majority of U.S. users are worried by the threats posed by AI, with one 2023 study from Morning Consult and Twitter showing 70% are concerned about its ability to spread misinformation. The same proportion are troubled by its use by foreign powers against U.S. interests, and 68% are worried about the creation of deepfakes.[25] Research undertaken by YouGov in the same year shows 78% of U.S. adults are either "very" or "somewhat" concerned about AI's use in spreading political propaganda,[26] making it imperative for policymakers to take a proactive stance in tackling these concerns.

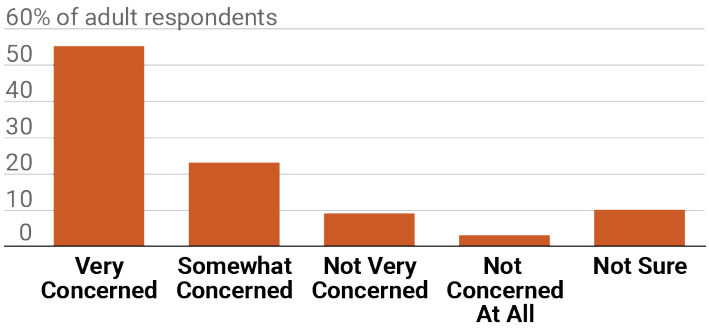
Scoring AI and Human-Generated Disinformation



Source: OECD

Concerns About AI Propaganda

Survey results of adults in the United States from 2023



Source: Statista

Data around the numbers of Americans who regularly fact-check is limited. The available information on the topic is generally either out of date, based on low sample sizes, or analyzes populations beyond the U.S. Nevertheless, there is evidence to suggest that U.S. citizens:

1. Have low confidence in their fact-checking abilities: A Pew study in 2020 found that 71% of people held low confidence in their ability to check information relating to COVID-19.[27]
2. Are often unable to locate the source of fake news: A survey of 3,446 people in 2019 found that 52% of respondents thought a fake video from Russia showed "strong evidence" of election fraud during the 2016 Democratic Party primaries. In addition, only three people were able to locate the true origin of the video.[28]
3. Visit untrustworthy websites regularly: A survey found 44% of people visited untrustworthy sites during the 2016 U.S. presidential election campaign. The authors defined such websites as "lack[ing] the news media's editorial norms and processes for ensuring the accuracy and credibility of information."[29]
4. Are more likely to trust fake news that aligns with their political views: A 2022 study of U.S. Democrats found that demand for fact-checking in a political newsletter rose when it contained information from Fox News. However, fact-checking did not have a significant impact on demand for the newsletter where information from MSNBC was included.[30]
5. Hold differing views of fact-checking: Conservative Republicans hold less favorable views toward fact-checkers, while people interested in and knowledgeable about politics tended to be more favorable.[31] Similar results have been found among Europeans. The data suggests those most at risk of believing fake news could be on the right and/or less engaged with the political process, although this conclusion is hotly debated.

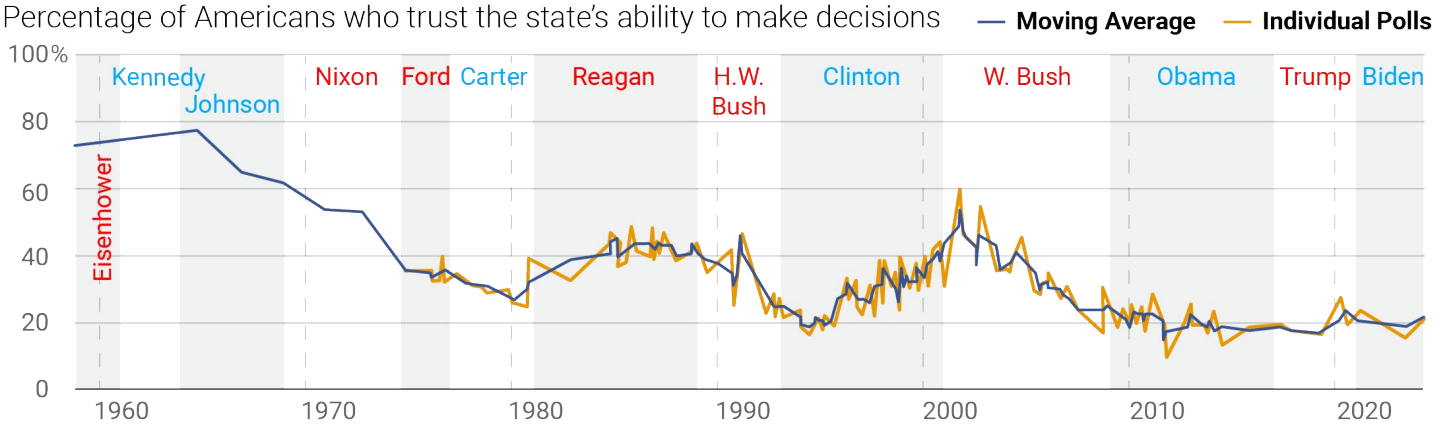
Taken together, these studies paint a picture of an American public ill at ease with differentiating truth from fabrication online. U.S. policymakers need to ensure the public is aware of the power of AI, or the outlook could become even more concerning.

The biggest threat of foreign influence campaigns is the ability to undermine trust in government and potentially stoke civil unrest. In 1964 trust in the U.S. government was at an all-time high. That sentiment underwent an alarming decline in over the next four decades, reaching historic lows in 2011.[32] That decline is not just a U.S. phenomenon. Distrust in government institutions internationally is a trend well-acknowledged by the United Nations[33] and the OECD.[34] It is difficult to draw a direct line between fake news from international influence campaigns and this trend, but it would be hard to argue that Spamouflage, or the alleged Russian-backed influence campaign called Doppelganger, do not add fuel to this fire in the U.S.

Another public policy challenge is the power of foreign influence campaigns to use fake news to fan the flames of quickly emerging national crises when information is scarce. For example, during the 2024 United Kingdom riots, or both the Pennsylvania and Florida assassination attempts on Donald Trump, fake news from a myriad of sources spread quickly. The power social media platforms hold in these cases is significant. Meta has an escalation process for restricting accounts of high-profile users during periods of civil unrest, given their potential to supercharge the spread of fake news.[35] In 2021, the company indefinitely suspended Trump's Facebook and Instagram accounts following his praise for people involved in the Jan. 6, 2021, assault on the U.S. Capitol and the alleged risks this posed for further violence. The suspension, which was later reduced to two years on the advice of Meta's Oversight Board,[36] was ultimately lifted in January 2023 with "guardrails"

Government Trust Falls to an All-Time Low

Percentage of Americans who trust the state's ability to make decisions



Source: Pew Research

and heightened repercussions for further violations. The restrictions were removed as presidential candidates geared up for their respective party conventions in 2024.[37]

Social media platforms walk a tightrope: For a pro-Trump Republican, the removal of a post about immigration that violates community guidelines might be considered censorship, but for a Democrat the same act might be viewed as a responsible reaction to inflammatory messaging. Oftentimes, moderating content involves a subjective assessment of the information in question, an assessment that Meta CEO Mark Zuckerburg recently called out as all too often being "politically biased", when he removed human fact checkers and replaced them with community moderation.[38] It can also include a more objective assessment of whether content violates a platform's user policies, which will have been established by consensus among a group of colleagues with subjective views.

Censorship arguments have divided U.S. lawmakers, society, and the social media platforms themselves. Platforms should not get Section 230 protection , which sees them given immunity for content published by users, if they censor online speech. Therefore, it is incumbent on all sides to find agreement in a unified goal: Tackling state-backed influence campaigns and fake news should be the objective, and achieving this requires close collaboration between the public and private sector. As a first step, Federal Communications Commission Chairman Brendan Carr, should undertake a review with platforms to understand how their policies are implemented in practice, including at times of national crisis.

The Double-Edged Sword

Technology's Role in Spreading Fake News

Beijing-linked organizations have been accused of using sophisticated technologies such as Synthesia[39] and CapCut[40] to create fake videos and OpenAI tools to undertake intelligence analysis.[41] OpenAI's Sora and Google's Veo 2,[42] generation models that create sophisticated moving images from language prompts and photos uploaded from a user, have the power to further supercharge the ubiquity of misleading footage originating aboard.[43] Gary Marcus, AI expert and professor emeritus at New York University, described the stark potential of AI tools to spread misinformation which in the worst case scenario could "lead to an accidental war that escalates and becomes a nuclear war."[44]

In 2023, the Australian Strategic Policy Institute uncovered a huge campaign of pro-China AI-generated YouTube videos it called " Shadow Play." At the time of publication, the campaign included "at least" 30 channels, over 4,500 videos, 120 million views and 730,00 subscribers."[45] Fake news from China is not confined to the most popular social media platforms; Spamouflage-linked accounts have also been detected on Bluesky and Mastodon. Closer to home , a disgruntled ex-employee of a Baltimore school was charged with spreading an audio deepfake falsely depicting the school's principal making racist

comments.[46] This case study has stark implications for the use of AI tools: Their ability to be used by non-specialists, their relative sophistication compared with only a few years ago, and their potential for generating community-level division. If such methods can be instigated by actors at home, it emphasizes their ability to be employed by an increasing number of untrained actors abroad.

The acquisition of sophisticated technology from overseas could enhance the ability of China-backed actors to spread fake news. However, U.S. authorities have tightened their grip on exports that help develop AI. The Foreign Direct Product Rule (FDPR), first established in 1959, has become crucial over the last decade in efforts to limit sensitive U.S. exports. In 2019, the Bureau of Industry and Security took action against Huawei, and then in 2022 wider controls were put in place on other Chinese companies limiting the transfer of code, electronics, chips, and supercomputing capabilities.[47] In the final days of the Biden presidency, the FDPR was further deployed to stop exports to a further 140 entities, with new controls on semiconductor manufacturing and software tools and the high-bandwidth memory crucial to training AI.[48] Alongside the U.S., other allies, including the United Kingdom,[49] the Netherlands,[50] and Japan[51] have passed rules with various success. When FDPR and international action is taken, technology companies often halt their dealings with Beijing. These moves have significant implications for China's ability to develop its AI sector and therefore create new technologies for propagating fake news.

However, U.S. policymakers need to analyze the effectiveness of the FDPR. Chinese companies and researchers can continue to make progress in their ability to spread fake news by circumventing technology bans.[52] ByteDance rents Nvidia chips via Oracle's U.S.-based operations, and there is a possibility Alibaba and Tencent may do the same.[53] Likewise, semiconductor intermediary dealers enable businesses in China to get around the controls by selling to the domestic market from third countries.[54] In addition, China has boosted subsidies to chip makers , restricted sales of critical minerals to the United States, and launched an antitrust investigation into Nvidia.[55] All the while companies based in the country, including Huawei, continue to make progress in their development of advanced semiconductors. Chinese large language models (LLMs) saw significant improvements in 2024, with the strongest ones produced by companies like DeepSeek, Alibaba, 01.AI and Zhipu AI, often with lower training cost than their US competitors.[56,57] If U.S. policymakers want to tackle the increasing role of AI in spreading fake news, it needs to review its response to these wider export and technology issues.

On taking office, Trump revoked Biden's executive order on AI,[58] claiming it hinders innovation,[59] replacing it with a new policy aimed at promoting "human flourishing, economic competitiveness, and national security."[60] Among a number of goals, the previous presidential order instructed the federal government to undertake work to "establish the authenticity and provenance of digital content," established chief AI officers in large agencies, and tasked providers of Infrastructure as a Service (IaaS) providers to submit to the Secretary of Commerce a report when a "foreign person transacts [with them] to train a large AI model with potential capability that could be used in malicious cyber-enabled activity." Goals such as these may have allowed federal authorities to identify fake news more easily and ensure state-backed actors are not using U.S. IaaS products to train AI technologies that enable this activity. Speaking at the Paris AI Summit in February 2025, JD Vance further reset U.S. government AI policy with a speech describing the technology's "revolutionary applications" to "free expression."[61] As part of its new action plan, the Trump administration will need to consider how a replacement mechanism can strike a balance by defending new U.S. technologies, ensuring national security, and promoting free speech.

Technology's Role in Combating Fake News

While Meta's former President of Global Affairs Nick Clegg pointed out it's still "early days for the spread of AI-generated content,"[62] public and corporate enthusiasm for generative AI tools has led to their quick development. This has created a huge amount of new content and the potential for orders of magnitude more. To realistically combat the potential flood of AI-generated false content, the quality and number of defensive AI tools able to mitigate fake news

Nick Clegg, president for global affairs at Meta, testifies during the Senate Select Intelligence Committee hearing titled "Foreign Threats to Elections in 2024 - Roles and Responsibilities of U.S. Tech Providers," on Capitol Hill on Sept. 18, 2024. (Tom Williams / CQ-Roll Call, Inc. via Getty Images)

needs to match the number and sophistication of the ones creating it.

Social media companies have a long history of utilizing AI classifiers to categorize huge amounts of content according to specific attributes to ensure it does not break community rules. However, when it comes to detecting fake news, the work of these classifiers often still needs to be completed by human review.[63] For example, a classifier might identify a post as misinformation, but what happens if the misinformation becomes factual truth later? Or what if a post is a joke from one user to another, or might be literally false but clearly understood by reasonable people as satire?

One solution can be found in the growing number of technologies that help uncover online information with dubious provenance. For example, the Coalition for Content Provenance and Authenticity (C2PA) standard, an alliance between Adobe, Arm, Intel, Microsoft, and Truepic, has created a specification for a cryptographically sealed manifest showing users' edits that have been made to photos, videos, and audio clips on the web.[64]

Another solution from Google called SynthID embeds a digital watermark directly into AI-generated images, audio, text, or video.[65] In the first of its kind, SynthID had been rolled into the Gemini LLM with watermarks generated alongside the response. This stands in contrast to traditional detection of AI-generated text that has taken place after it has been created. Researchers at Google found that SynthID has minimal impact on computational power and enables "better detectability"[66] than other watermark technology. Google has since released the solution as open-source code.

Efforts such as C2PA, SynthID, and social media platforms' periodic attempts to remove fake news may not be able to stem the tide. In addition to these solutions, no AI-enabled fact-checkers, from organizations such as U.K.-based Full Fact and Germany-based Factinsect, have received the levels of funding and public engagement needed to tackle the

spread of large quantities of fake news online. Much of the fact-checking around the 2024 presidential election continued to take place manually.[67] The idea of moving to an AI-first approach in the short term is implausible. However, public understanding and interaction with tools like C2PA, SynthID, and fact-checkers needs to increase significantly if U.S. policymakers want to tackle fake news seriously.

Foreign actors may not want to implement new transparency measures such as SynthID into their own LLMs. There is also an inherent risk that LLMs themselves are trained on data that itself includes fake news. In China alone, there were reportedly over 180 government-approved LLMs in 2024,[68] but the total number created by Chinese actors is likely to be much higher and growing all the time.

Three solutions might be appropriate as an interim solution while the adoption of defensive AI tools gathers momentum:

1. Better utilization and more research and development around retrieval-based approaches, where a record is kept of known AI-generated text, or post-hoc detection systems, which can detect such text after creation.
2. A meta-analysis to establish and quantify in a more robust way the scale of the problem. For example, social media platforms could introduce dashboards showing the levels of information being published that does not include visible watermarks, or which has edited provenance. This approach would become increasingly beneficial as watermarks are rolled out, while also showing users the existing underutilization of these technologies to date. Eventually these dashboards and meta-analyses must be as easily accessible to the consumer as the generative tools, avoiding the need to rely on experts, law enforcement, or academia for information.
3. Better access to platform APIs to allow researchers access to the data that may help analyze the impact of fake news. The European Commission's request for information from Meta, to ensure it is complying with the Digital Services Act's (DSA) requirement to give researchers easy, real-time access to data that might improve transparency around malicious online political content, is a first step toward international action.[69] U.S. policy makers should consider how they are pushing companies towards best practice too.

Inspiration should also be sought from Bill Gates, who is among the world's most affected targets of conspiracy theories.[70] The former Microsoft CEO has been the subject of many fake news campaigns, notably in relation to health, climate, and vaccine rollouts. For example, in 2024 a story that he had funded research into genetically engineered cattle ticks gained traction online. Gates has his own dashboards that scrape platforms for mentions of conspiracies in relation to him. Information is given on the percentage change in mentions of each inaccurate claim, as well as their reach.[71] They allow him to drill down into the detail of an individual post and track its origins. Such solutions are not out of reach: Many social media monitoring technologies track online conversation, including Sprout Social, Hootsuite, and Brandwatch. These tools can be used to identify authorship, discover who has shared posts, and analyze public sentiment[72] toward the content. Taken together these abilities can deepen the public's understanding of fake news on their social media feeds. For example, a user might be more skeptical of content that had been posted and spread from China with a negative tone toward the United States. Social media platforms could do more to ensure this information is available to users without having to use one of these third-party providers.

Academia is also leading on a number of initiatives to stop the propagation of fake news. SimPPL, a research collective from the Massachusetts Institute of Technology, creates open-access tools and new research to boost online transparency. The team has delivered an engineering framework to visualize social media interactions, evaluated the impact of LLMs in online hate speech, analyzed Chinese actors' online activity with Meta, and undertaken analysis of Reddit algorithms' ability to direct users toward fake news. They are currently undertaking a project to evaluate LLMs' propensity to share fake news and the implications of deepfakes on election integrity.[73] Is That True?, a project from the University of São Paulo, has created a chatbot on Telegram and a web-based app to help users detect fake news. The team claims over a 95% accuracy on training data and 70% accuracy on real world news.[74] The platform was

trained using the LIAR dataset, which helps develop fake news detection machine-learning algorithms.[75] Finally, researchers from Arizona State University have created a new audio deepfake detection method that measures biosignals like the vibration of vocal cords in the throat and mouth. These are then compared to the speech acoustics of the recording to confirm a common human origin with an error rate of less than 0.004%. Once recorded, audio is watermarked or cryptographically signed, confirming its genesis is authentically human and not AI.[76]

U.S. policymakers should recognize the importance of this work in repelling fake news from China and elsewhere by ensuring it is well-funded. In addition, the latest technologies that have passed peer review should be quickly incorporated into the approach of both government agencies and social media platforms to ensure powerful new technologies are not confined to academic "ivory towers." Given the fast-moving nature of developments in the sector, the government needs to improve its active engagement with the academic community tackling fake news. Ultimately, if this battle is to be won, U.S. policymakers need to embrace these new and existing technologies with the same enthusiasm the public has given to generative AI.

Social Media Algorithms

Each algorithm is a powerful unique technology. Platforms understandably need to provide users with content they find interesting, and many of their business models rely on constant user engagement. But this often traps users in "echo chambers" that reinforce a user's impression that the whole platform subscribes to their own beliefs. Often these echo chambers will contain significant amounts of fake news. This could mean that if a person is interested in conspiracy theories related to "chemtrails," there is a higher likelihood they will thereafter be shown information about alleged coverups related to 9/11, or QAnon content. Renee Diresta, a leading expert on fake news, [77] compares the effect to that of a murmuration of starlings. If one changes direction, it has a cascading effect in which the rest of the flock changes directions, too. But no one bird can see the knock-on effect it is having.[78] In the same way, an apparently innocuous share of a post or like of a page containing fake news has wider significance.

Given the power of these algorithms, more should be done to scrutinize how they work. The DSA gives EU member states the power to compel large platforms to provide access to their algorithms,[79] and the European Commission has opened investigations of both Meta's and TikTok's underlying algorithms.[80] In the U.S., the issue has been dealt with on a case-by-case basis, involving a myriad of lawsuits that challenge the algorithms used by TikTok, Google and Meta through the courts.[81] In one case against Meta, a coalition of attorneys general claim the company has set out to "purposefully addict children and teens."[82]

Following these lawsuits and the European Commission's interventions on the other side of the Atlantic, lawmakers should undertake a formal assessment. The spread of fake news online is an inherently cross-border issue; a false story seeded in China can reach U.S. users in seconds. A regulation or directive in Europe impacts users across the Atlantic. How fake news is dealt with depends on the legislative and cultural contexts of those countries, and therefore U.S. policymakers may not support Brussels' interventionist approach with legislation like the DSA. However, they should not ignore the findings of international investigations and legal mechanisms that may directly impact U.S. users too.

China's Link to U.S. Fake News

COVID-19 and Elections

The 2010-2012 Arab Spring marked a tipping point in which governments across the globe, from authoritarian regimes to democracies, realized the capability of the internet and specifically social media to deliver regime change.[83] The use of social media platforms during the protests played a multifaceted role , by making citizens "better informed, turning them into activists, facilitating public organisations and collective action, and eventually helping the development of democratic institutions that could replace autocratic regimes."[84] In the decade and a half since Mohamed Bouazizi's self-immolation catalyzed the movement, governments have responded by taking a more proactive stance in using the internet to assert their national and international geopolitical priorities. This activity covers the spectrum from truthful updates to inform the public, on to national propaganda, then

ending with some of the worst examples of fake news spread abroad.[85]

Two sets of issues have helped fuel online fake news more than any other: COVID-19 and events leading to the riot at the U.S. Capitol on Jan. 6, 2021.

Beijing-linked actors' role in spreading fake news during the height of the pandemic and afterward are well-researched.[86,87] In the early stages of the crisis, accounts linked to China downplayed its seriousness, called the virus' origins into question, proposed unscientific treatments, and questioned the efficacy of FDA-approved vaccines. In one piece of analysis over the course of nine months, the Associated Press and the Atlantic Council's Digital Forensic Research Lab found examples including the People's Daily, the country's official newspaper, "highlighting speculation" that the U.S. military brought it to China[88] and the foreign ministry broadcasting a conspiracy video claiming the virus was a U.S. biological weapon.[89] The impact on people's behavior of fake news during the pandemic is less understood, but sources including the World Health Organization and individual physicians have claimed material impacts.[90,91] By June 2020, online misinformation had inspired over a dozen people to swallow disinfectant, believing it would prevent infection. Disinformation also arguably led to unnecessary panic buying.[92] Other theories, including that powerful elites had intentionally planned the outbreak,[93] or that the threat had been exaggerated to damage Trump,[94] were also common online narratives.

While China did not attempt to explicitly influence the 2020 presidential election , the vote marked the start of a Spamouflage "breakout" of China linked-actors, according to researchers at Graphika. [95] Spamouflage was quick to react to the attack on the U.S. Capitol, with the network promoting footage of the riot with mentions of "civil war."[96] One video with links to China claimed to show someone burning ballots in Virginia, footage that was shared by Eric Trump in a post that received 1.2 million views.[97] Much of the content was amplified, perhaps unknowingly, by the official accounts of Chinese diplomats who may have been influenced by traditional media. For example, in the runup to the vote, a Chinese news website was accused of splicing "Hunter Biden material with easily provable false information,"[98] while other

Democratic Rep. Eric Swalwell reacts to a GOP member's post on X utilizing A.I. generated imagery during a House Judiciary Committee hearing about open border policies on Sept. 10, 2024, in Washington, D.C. (Tom Brenner / Getty Images)

outlets painted the attack as a result of "U.S. Society's severe division."[99]

Most recently, a September 2024 Graphika report found evidence of a Chinese "state-linked" influence operation ahead of the 2024 presidential election,[100] marking a departure from the NIC's assessment of the 2020 vote.[101] The report found that Spamouflage-linked accounts had "seeded and amplified content denigrating Democratic and Republican candidates, sowing doubt in the legitimacy of the U.S. electoral process, and spreading divisive narratives about sensitive social issues including gun control, homelessness, drug abuse, racial inequality, and the Israel-Hamas conflict."[102] A Microsoft analysis of Storm 1376 – its term for Spamouflage – found attempts to push "key issues that divide U.S. voters" in the runup to the vote by posing contentious questions on controversial domestic issues.[103]

To understand behaviors indicative of the Spamouflage network, we can assess the "Three As": activity, anonymity, and amplification, a method often used to identify bot networks.[104] These attributes can be tracked with analysis of social media networks.

On the basis of such research, Spamouflage accounts tend to feature:

1. **Activity:** Posts are often made either in inaccurate English or in Chinese. Often the content attacks Western political figures, mentions divisive issues in other countries, or promotes conspiracy theories. Additional content often describes Chinese politics and society in positive terms. Cultural references including important national symbols, events, and locations are often posted. Sometimes accounts are operated by a central actor that is automating activity. These accounts have standardized posting schedules or a quantity of posts far exceeding the rate of a normal human user.
2. **Anonymity:** Profiles can feature vague or nonexistent biographical information, making it impossible or difficult to identify the author. Sometimes profile pictures include a Chinese national emblem or an inauthentic image of a person who does not appear to be of Han Chinese ethnicity.
3. **Amplification:** Accounts with the above activity and anonymity features tend to repost each other, follow each other (so-called "follow back" behavior) and engage with prominent accounts from social media influencers and high-profile political figures in the West. Much of the content can be unoriginal and shared across multiple accounts.

On Nov. 5, 2024, accounts displaying these characteristics pushed narratives discrediting the presidential election result and amplifying anxiety about potential violence. One described the vote as a "money-burning war" in reference to the fact that U.S. elections are among the most expensive in the world.[105] After the election, a prominent post featured a cartoon from an influential pro-China artist showing Trump and Kamala Harris as puppets controlled by corporations (see Figure 4). Others posts ridiculed Harris, claiming she was "dog-walked" by Trump.

Showing the Link

Microsoft analysis shows that China employs over 230 state media employees and affiliates who "masquerade as independent social media influencers across all major Western social media platforms."[106] This has parallels to a recent Russian campaign, uncovered by the Department of Justice and other agencies,[107] that paid western influencers to spread propaganda , which they claim they were doing unwittingly.[108] In the same way, the DOJ, FBI and wider intelligence community needs to publicly demonstrate how the Chinese state is directly responsible for fake news, rather than private Chinese citizens or entities.

This can be done with direct attribution using IP addresses or indirect attribution using geotagging or cookies. Other techniques, such as analyzing the Three As, have proved helpful. Despite these methods , the Chinese government routinely denies accusations that it runs influence campaigns targeting other countries. When accused of an online influence operation during the 2024 presidential campaign, a Chinese Embassy spokesperson said: "China has no intention and will not interfere in the U.S. election, and we hope that the U.S. side will not make an issue of China in the election."[109] When the nonprofit Network Contagion Research Institute accused TikTok of presenting information to users that gave an unequally positive view of China, a Washington-based embassy spokesperson issued a similar denial, saying the report "has no factual basis and is full of prejudice and malicious speculation."[110] Questioning the factual basis of research is a common response from Chinese embassies when responding to accusations.[111]

On the face of it, China can point to its own tough domestic laws on the spread of fake news by citing numerous pieces of legislation.[112] The Cyberspace Administration of China bans AI-generated images and video without a watermark. The Economist points out that while the Chinese Communist Party tackles "genuine misinformation," they also "label anything that contradicts the party line as such."[113]

TikTok

While national security concerns are paramount, there is also a public interest in understanding the link between China and fake news in more detail. Nowhere is this more reasonable than with the example of TikTok, which as of 2024 has around 170 million U.S. users. The bill that would ban the app in the U.S. has thrust the issue into the spotlight.[114] During TikTok CEO Shou Zi Chew's appearance before Congress in March 2023, U.S. Sen. Ted Cruz highlighted China's 2017 National Intelligence Law, which sets out that "all organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national

> "In exerting control over Chinese parent companies through formal legal means and, more frequently, the informal business culture that surrounds the PRC's legal framework, the PRC can access information from and about U.S. subsidiaries and compel their cooperation with PRC directives."
>
> **Kevin Vorndran**, assistant director of the FBI's Counterintelligence

intelligence work secrets they are aware of."[115] Chinese laws such as these are often given as evidence that Beijing is able to implement foreign influence operations through direct engagement with its society, a power that has no equivalent in the U.S.

In *TikTok v. Garland*, the case brought by the social media giant to challenge the bill, the DOJ laid out the risks posed by the app. But much of the government's July 2024 filing to the Court of Appeals for the District of Columbia was redacted.[116] Lawyers cited national security concerns for the withheld information.[117] A similar point was made by U.S. Rep. Josh Gottheimer, who drafted an earlier bill to ban TikTok, when he said, "we have seen evidence [about TikTok] in a classified setting."[118]

Currently, users understand only the broad nature of the connection. For example, in the July 2024 filing, Kevin Vorndran, assistant director of the FBI's Counterintelligence Division, laid out[119] the undetailed argument government officials often make in public forums:

> "In exerting control over Chinese parent companies through formal legal means and, more frequently, the informal business culture that surrounds the PRC's legal framework, the PRC can access information from and about U.S. subsidiaries and compel their cooperation with PRC directives. In contrast, in the United States, U.S. subsidiaries are generally treated as U.S. persons and afforded robust legal and constitutional protections."

David Newman, principal deputy assistant attorney general of the National Security Division of the DOJ,[120] concurred in the same filing, mentioning laws that "blur the line" between the public and private sector in a way that was "very different" to the way private companies operate in the U.S.

While public statements such as those from the FBI and DOJ are helpful to an extent to understand the nature of Chinese influence, when we look at the insufficiencies of TikTok's proposals to placate[121] the federal government, we are literally reading between the lines of a heavily redacted document.[122] The intelligence community needs to publicly demonstrate more clearly how the Chinese state is directly responsible for fake news, rather than Chinese citizens or private entities.

FARA

China's Global Television and its Xinhua News Agency and network were required[123] to register as foreign principals[124] under the Foreign Agents Registration Act (FARA),[125,126,127] and did so in 2019 and 2021 respectively. The law was introduced in 1938 to combat the rise of German propaganda before World War II.[128] As the DOJ looks to FARA as a tool to counter propaganda from abroad, we can perhaps look at it as a tool to tackle fake news too. The lines between state-sponsored propaganda and fake news are often blurry. Arguably, the two can in many instances be one and the same: Some of the content published by Chinese social media accounts that have spread falsehoods about Maui wildfires and the federal government's poisoning of other countries' water supplies[129] might fit into the definition of "political activities" under FARA.[130]

In September 2024, an alleged agent of Beijing, Linda Sun, was indicted on charges of violating FARA as part of her work with New York Gov. Kathy Hochul.[131] We

might need to consider the real possibility of Chinese-backed individuals being charged under FARA for online influence campaigns too.

A precedent has been set by Russia's attempt to influence U.S. political life through online activity. The day after the news about Sun broke, two RT employees were indicted under FARA related to "a $10 million scheme to create and distribute content to U.S. audiences with hidden Russian government messaging."[132] In coordinated government action, 10 individuals and two entities were sanctioned[133] and 32 internet[134] domains were seized as part of an investigation into the Russian Doppelganger program. This follows the 2018 grand jury indictment of 13 individuals as part of then-Special Counsel Robert Mueller's work on Russian interference during the 2016 presidential election.[135] The charges against the individuals were not formally dropped[136] and they have not been extradited by Moscow. The possibility that Beijing-backed individuals will face similar charges is perhaps the next milestone following China's well-known attempts at what the DOJ describes as "state-sponsored"[137] hacking as well as other infiltration attempts.[138] Given the experience with Doppelganger, U.S. policymakers should ready themselves for a similar moment with regards to Spamouflage so they can formulate a quick and effective response.

Part of the solution could be found in requiring certain agents[139] of foreign principals to flag their accounts and posts on social media. Under the terms of the act, the DOJ requires any activity undertaken within the U.S. to be reported. In recent opinions, the government has been expansive in its view on what this means, in one case saying this element was met because a foreign principal's online account was "clearly viewable in the United States."[140] Prior to the presidential election the DOJ promised to provide "more specific" guidance on labelling social media posts.[141] Attorney General Pam Bondi should build on this record by considering how her office can use the Act further. In a February 2025 departmental memo after taking office, she called for FARA to be used for "alleged conduct similar to more traditional espionage by foreign government actors," which suggests she may take an approach that does not recognize its potential for countering fake news.[142] An ambitious move would be for the new administration to instead propose social media companies proactively label suspected foreign-origin social media accounts under FARA with a precautionary principle-style approach. The user could later challenge the decision under a dispute resolution mechanism if they had been wrongly labeled.

Protecting First Amendment Rights

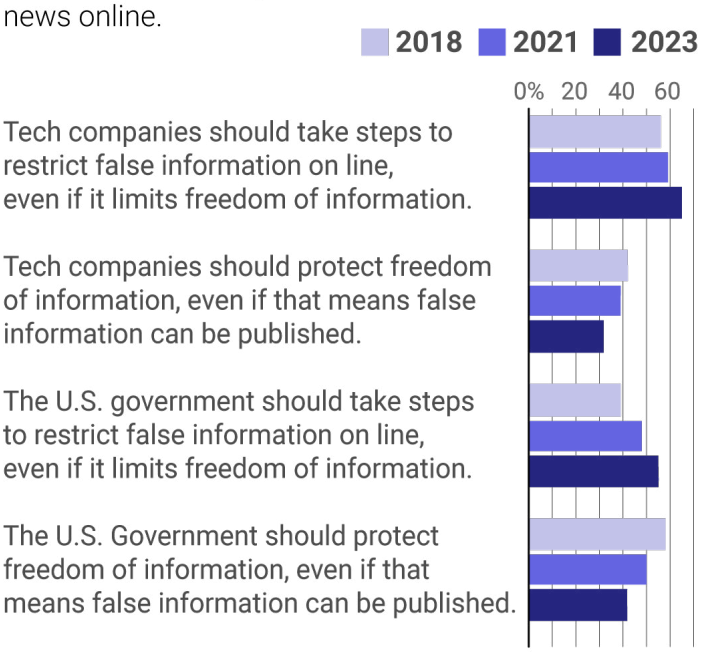
The countering of fake news from abroad must take First Amendment considerations into account. There should be a focus on checking facts without policing opinions. It is a common argument that the Bill of Rights applies to foreign nationals for conduct that takes place in the United States. The question arises whether foreign actors spreading fake news via U.S. servers therefore enjoy the protections afforded under the First Amendment.

During the *Murthy v. Missouri* case, which was decided by the Supreme Court in June 2024, the Biden administration argued it was legitimately liaising with platforms to tackle the spread of misinformation in relation to COVID-19 and elections. Then-Missouri Attorney General Eric Schmitt saw it differently, arguing government officials were "coerc[ing]" or "significantly encourage[ing]"[143] social media companies to remove views they disagreed with. This aligns with the views held by the new Trump administration. Speaking at the Munich Security Conference, Vice President J.D. Vance described how the previous administration "threatened and bullied" platforms to "censor so-called misinformation."[144] As a first step, U.S. Attorney General Pam Bondi disbanded the FBI's Foreign Influence Taskforce, which led much of the work to liaise with platforms. In her February 2025 memo, Bondi justified the decision due to the need to "free resources to address more pressing priorities, and end risks of further weaponization and abuses of prosecutorial discretion."[145]

Despite the U.S. Supreme Court's 6-3 decision favoring the Biden administration in *Murthy v. Missouri*, the issue is not settled because the majority said states had failed to establish standing[146] to sue the government as they were not able to identify "any specific speakers or topics that they have been unable to hear or follow" as a result of government action.[147]

Restricting False Information

Percentage of Americans who trust tech companies and the state's ability to make decisions about false news online.



Source: Statista

However it is notable that while the July 2024 preliminary injunction, which started the legal process toward the Supreme Court in *Murthy v. Missouri*, effectively halted much government liaison with social media companies, Judge Terry Doughty included exceptions[148] for national security, security threats, criminal efforts to suppress voting, and foreign attempts to influence elections. This exception for issues pertaining to international influence is telling. Foreign influence should warrant special treatment. Nevertheless, what constitutes international influence is inherently complex and requires close liaison and exchange of expertise between intelligence agencies and platforms. Despite this there remain important and legitimate voices who, as described in Supreme Court Justice Samuel Alito's dissent in *Murthy v. Missouri*, believe the government was putting "unrelenting pressure" on platforms "to suppress Americans' free speech."[149]

There is a risk international influence could increase dramatically if a heavy-handed attitude to fake news is now taken. U.S. lawmakers need to work out an approach that recognizes the complexity involved in analyzing sources of fake news, which could originate as part of a foreign influence campaign or have been seeded by domestic actors. This approach needs to balance the robust protection of the First Amendment with an equally robust defense against foreign influence. Ultimately, U.S. lawmakers need to decide a complex trade-off about whether they agree or disagree with a blanket right to free speech even when U.S. users are spreading fake news that has been seeded as part of a foreign influence campaigns. This is particularly true given research from Pew shows growing public approval for tech companies and government to limit false information online, even if it means limits to freedom of information.[150,151]

Recommendations

Throughout this report, several recommendations have been made specifically in relation to managing the spread of fake news from China. To summarize, U.S. policymakers should:

1. Recognize that Spamouflage is the largest cross-platform covert influence operation in the world.
2. Take the threat of Spamouflage more seriously given recent influence attempts during the 2024 presidential election, rising geopolitical competition with Beijing, and the growing technological sophistication of Chinese actors.
3. Use the precedent set by Russian online campaigns such as Doppelganger as a guide to what the future might hold for the threat posed by Spamouflage.
4. Demonstrate more readily the link between Spamouflage actors and the Chinese state. The DOJ's operation to expose the Russian government-sponsored disinformation campaign in 2024 could serve as a guide.[152]
5. Ensure the government has understood properly the limitations of the FDPR in limiting China's AI development and undertake work to close loopholes.

In addition, this report makes recommendations that have broader implications for managing the spread of fake news from all state-backed actors. To summarize, U.S. policymakers should:

1. Account for the U.S. public's difficulty in discerning truth from fake news and how to properly fact-check claims made online.
2. Work with social media platforms to understand the implementation of their user policies, particularly during times of national crisis.
3. Take a balanced approach that both supports the First Amendment and ensures platforms and agencies are able to counter international influence campaigns.
4. Consider how Trump's invalidation of Biden's executive order on AI and Bondi's disbandment of the FBI's Foreign Influence Task Force might impact the federal government's ability to counter the spread of fake news.
5. Encourage the private sector to develop defensive tools and technologies that can detect and stop the issue. These include access to public dashboards that give metrics on the provenance of posts, support to organizations developing technologies such as AI fact-checkers and watermark technologies, and pushing platforms to give wider access to data on fake news for users and researchers. These tools should be embraced with as much vigor as the public has given to generative AI.
6. Improve engagement with and funding for the academic communities studying fake news and the technologies that can tackle it. Task government agencies to rapidly incorporate the latest peer-reviewed tools into their attempts to counter fake news.
7. Undertake a formal review of findings following recent lawsuits against big tech companies in the U.S. and European Commission action in Brussels.
8. Consider how existing legislation such as FARA might be used to tackle fake news.

Finally, three additional detailed recommendations described below further support transparency, improve awareness of fake news, and help emerging platforms address the problem.

A State-Funded Fact-Checking Panel

U.S. work to combat fake news has been led by the Cybersecurity and Infrastructure Security Agency (CISA) and other partners such as the FBI. During election cycles, the National Association of Secretaries of State (NASS) and the Election Assistance Commission (EAC) also play a role. In 2020, a process was put in place[153] that allowed U.S. election officials who spot fake news to report it directly to the Elections Infrastructure Information Sharing and Analysis Center, a partnership among the CISA, the Center for Internet Security, and the Election Infrastructure Subsector Government Coordinating Council.

In the United Kingdom, the Counter Disinformation Unit was established in 2019 and makes referrals to platforms in cases of state-backed disinformation campaigns.[154] In France, VIGNIUM was established in 2021 to detect and deter foreign influence campaigns.[155] In Australia, the Electoral Commission established a register of "prominent pieces of disinformation"[156] during the 2022 federal election. In the EU, the DSA means that large platforms could face fines of up to 6% of their annual turnover if they do not take action to prevent manipulation of elections and disinformation.

When it comes to state-backed influence campaigns, intelligence organizations often discuss, analyze, and counter fake news away from public view in direct collaboration with platforms. Much of this secrecy is understandable due to national security concerns. But in the U.S., this gives rise to concerns about the implications for free speech, as seen in the case of *Murthy v. Missouri*.

A problem in virtually all jurisdictions is that organizations seeking to tackle fake news and foreign influence campaigns are spread across a myriad of different departments and agencies with different interests, roles, and responsibilities. At the same time, private sector fact-checking organizations often use different methodologies, lack public awareness, or are accused of being politically biased. The process of uncovering fake news therefore needs a figurehead organization with better public engagement, clearer transparency, political buy-in from both Republicans and Democrats, long-term funding certainty, and complete impartiality.

One solution could be a state-funded fact-checking panel researching the most egregious cases of

fake news propagation. Like many existing private sector fact-checking organizations, it could publish its findings, which would include the true sources of information and clarifications. To ensure neutrality, it might need to sit separately from the three branches of government. Membership of such a panel could be drawn from the public, legal experts, data analysts, Republican and Democratic lawmakers, issue-specific experts, and fact-checking organizations. The panel could hear cases brought from lawmakers, the government, platforms, and users, including those related to foreign influence campaigns. Once the panel's findings were made public, it would be up to the wider system to act.

The panel should be as transparent as Meta's Oversight Board, which publishes all its decisions[157] and recommendations[158] online for public scrutiny. However, the Board's role differs from that of the proposed panel in a number of key ways: It makes binding decisions on cases related to the Meta's user policies and proactive nonbinding recommendations to the company too, including in relation to misinformation. But the investigative nature of the board, the expertise of its members, its ability to hear diverse cases from different sources, and its transparent approach have made it a success.

The panel should be tasked with checking facts behind stories, not individual opinions. For example, Trump's claim that he won the September 2024 presidential debate, despite a flash poll suggesting Harris was more successful,[159] would not be a topic for the panel. However, his claim that migrants in Springfield, Ohio, were eating dogs, or comments in early 2025 about President Zelensky of Ukraine's approval ratings, might be.[160] Likewise, Joe Biden's claim that he "inherited" a 9% inflation rate on taking office,[161] or Kamala Harris' assertion that Trump would sign a "national abortion ban," or that unemployment was at its "worst since the 1930s" during Trump's previous tenure, could also be issues for analysis.[162] Fact-checking around milestone events, such as presidential debates, times of national crisis, and major speeches would be particularly important.

The panel's research would also help the wider system understand if the author was spreading misinformation or disinformation. For foreign influence campaigns this would be an important distinction given many state-backed actors would know the information they are spreading to be untrue. The panel would need the resources to move quickly, for example during periods of civil unrest, but also space to undertake longer investigations for complex or high-profile cases. It could operate with a digital first approach, with members of the public having the ability to vote on content to be reviewed.

A Government-Led Awareness Campaign

Government has a rich history of promoting information campaigns aimed at improving the lives of citizens by promoting smoking cessation, healthier eating, and the wearing of seatbelts. Examples include the Centers for Disease Control and Prevention's "Tips from Former Smokers" campaign,[163] the Department

Maricopa County election workers prepared for another onslaught of conspiracy theories in the 2024 by bulking up security and giving public tours of their ballot tabulation facility, (Patrick T. Fallon / AFP / Getty Images)

of Health and Human Services' "Risk Less. Do More" vaccines campaign,[164] the National Highway Traffic Safety Administration's "Click it or Ticket" seatbelt campaign[165] and the Department of Agriculture's "MyPlate" healthy eating campaign.[166] There have also been campaigns involving partnerships between the government and private sector, such as those focused on combating sexual assault on college campuses[167] and raising awareness of the impacts of illegal narcotics.[168]

The communications campaign to tackle fake news, however, has been a complex and overlapping effort by a range of government and nongovernment actors. Prior to the 2020 election, CISA operated a "rumor control"[169] and the NASS ran a #TrustedInfo2020 campaign. Four years later, the campaign was renewed, and other activity, such as an FBI and CISA joint public service announcement in September 2024, published a number of recommendations.[170] The impact of these campaigns in tackling fake news and increasing public understanding is unclear. They also have a wide variety of different messaging strategies, products to assist users in combatting the spread of fake news, and target audiences. This creates an unnecessarily complex set of messages for the public.

Drawing upon the experience of NASS, EAC and CISA, the U.S. government could act to bring together divergent strands into a single aligned campaign encouraging the public to do their own research. It could be targeted toward a number of "supersharers" who are responsible for spreading the majority of misinformation.[171] Given that fake news touches a range of policy areas and departmental portfolios, this campaign might have to be led directly from the White House. Alternatively, new remit could be given to the FCC as part of its broader responsibility for strengthening the nation's communications infrastructure.

The campaign could focus on the concept of prebunking,[172] which makes people aware of fake news before they encounter it, equipping them with the tools, techniques, and skeptical mindset needed to face these challenges in their day-to-day lives. One approach to making this message resonate would be to gamify the concept of prebunking.[173] U.S. authorities could build on the work undertaken by scientists at the University of Cambridge, who found that playing an interactive game called Bad News exposed participants to "weakened doses" of misinformation techniques that made the them subsequently "rate fake news as significantly less reliable after the intervention."[174] They found that this so-called "inoculation effect" of playing the game remained "stable" for at least three months.[175] Inspiration could be sought from a publicly available game drawing upon these learnings called Go Viral!, which was built by a team at Cambridge with the U.K.'s Cabinet Office in order to tackle misinformation in relation to COVID-19.[176]

Support for New Platforms

Virtually all online information platforms that claim to minimize the influence of algorithms on the user are small, with notable exceptions like Bluesky , Signal, and Mastodon. There are a myriad of other networks that claim to prioritize unfiltered content, including BeReal, Vero, Diaspora, and trustcafe.io. Some allow users to subscribe to feeds, effectively allowing them to opt out of receiving content. Others show users a stream of content, for example in chronological order, meaning they could view information from diverse sources, or only allow engagement between friends, or are messenger apps, for which in both cases the user has the power to engage with people or organizations of their own choosing. Despite the existence of these challenger brands, the biggest social media networks in the U.S. rely on algorithms to deliver a personalized experience. Eliminating algorithmic content entirely would destroy their business models.

By the same token, social networks that prioritize user choice in the content they view can be at an inherent financial disadvantage, but Bluesky, Signal and Mastodon show that strong user bases can be built. These networks are often organized around closed communities such as a Signal group, or a Mastodon private server. Bluesky allows users to select their own algorithm.[177] While fake news can appear on these networks, its spread can be contained to an extent by the walls users themselves organize around their communication and their ability to actively select the content that is shown to them.

Regardless of whether a new platform prioritizes algorithms or not, support needs to be given to new entrants that set tackling of fake news as their core mission. A new company could automatically label digitally altered content during sensitive election periods, as mandated by California's new deepfake law.[178] Or it could provide users with easily accessible dashboards showing the spread of fake news, or metrics on which posts have been shared by whom. If both sides of the aisle agree that fake news can damage society, they need to support new companies that allow users to avoid the worst echo chambers. This could also be achieved through better signposting to government support – for example with loans guaranteed by the Small Business Administration, state-level grant programs,[179] federal grant programs,[180] and tax credits.

Another approach might be to put in place a voluntary open algorithm commitment, in much the same vein as the AI commitment published by the previous White House administration, which major companies like Google, Anthropic, and OpenAI signed.[181] This commitment could outline guarantees such as to develop algorithms in a more transparent manner and prioritize research on societal risks. This would assist both the government and public in understanding how fake news could spread on social media. In addition, the executive branch could run a red-teaming exercise of algorithms, like the ones run with AI companies to analyze AI risks in 2023.[182] This exercise could identify algorithms that are most effective in stopping the spread of fake news and this would produce powerful learnings for both established and new platforms. Finally and importantly, all lawmakers should actively speak up in support of new emerging platforms as powerfully as they have in condemning the spread of fake news.

Sam Douglas-Bate is an expert on misinformation and disinformation in the modern age. Prior to establishing ForgeFront, a policy and futures consultancy, he worked for the UK Government at the FCDO and Cabinet Office. An accredited data analyst, he has led complex projects in the public and private sector related to technology, security and defence.

Endnotes

1 Watson, A. (2024, April 17). Frequency of seeing false or misleading information online among adults in the United States as of April 2023, by age group. statista. https://www.statista.com/statistics/1462057/false-news-consumption-frequency-us-by-age/

2 Wendling, M. (2024, November 3). Whirlwind of misinformation sows distrust ahead of US election day. BBC. https://www.bbc.com/news/articles/czj7eex29r3o

3 Federal Bureau of Investigation. (2024, November 4). Joint ODNI, FBI, and CISA Statement [Press Release]. https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-110424

4 Office of the Director of National Intelligence. (2024, November 1). Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts [Press Release]. https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/4014-pr-28-24

5 National Intelligence Council. (2021). Foreign Threats to the 2020 US Federal Elections (Report No. ICA 2020-00078D). https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

6 Microsoft Threat Intelligence. (2024, April 4). Same targets, new playbooks: East Asia threat actors employ unique methods. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/east-asia-threat-actors-employ-unique-methods#section-master-oc526b

7 https://scontent.fbrs4-1.fna.fbcdn.net/v/t39.8562-6/10000000_878173163681285_2523028760863660247_n.pdf?_nc_cat=100&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=G7cDZGZRyN0Q7kNvgHL7iZJ&_nc_zt=14&_nc_ht=scontent.fbrs4-1.fna&_nc_gid=AGoDLE2OIiO8M66x4mjml2A&oh=00_AYAyy9ydEaaHzlNil5PDwyRpA6-EQitOOH4yJIy21E2oKA&oe=6736D308

8 The next American president will be a China hawk. (2024, October 10). The Economist. https://www.economist.com/united-states/2024/10/10/the-next-american-president-will-be-a-china-hawk

9 Cybersecurity & Infrastructure Security Agency. (2024, October 25). Joint Statement by FBI and CISA on PRC Activity Targeting Telecommunications [Press Release]. https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-prc-activity-targeting-telecommunications

10 Li, J. (2019, August 27). Conflict Mediation with Chinese Characteristics: How China Justifies Its Non-Interference Policy. Stimson https://www.stimson.org/2019/conflict-mediation-chinese-characteristics-how-china-justifies-its-non-interference-policy/

11 Permanent Mission of the People's Republic of China to the United Nations and Other International Organizations. (2023). US Hegemony and Its Perils. https://archive.is/uQSsg

12 U.S. Department of State. (2023, March 14). The Kremlin's Never-Ending Attempt to Spread Disinformation about Biological Weapons. https://www.state.gov/the-kremlins-never-ending-attempt-to-spread-disinformation-about-biological-weapons/

13 Bing, C., & Schectman, J. (2024, June 14). Pentagon ran secret anti-vax campaign to undermine China during pandemic. Reuters. https://www.reuters.com/investigates/special-report/usa-covid-propaganda/

14 Graphika. (2024). Pro-China Accounts Leverage Cartoons to Target Philippines, Blame US for South China Sea Disputes. https://launch.graphika.com/pro-china-cartoons-south-sea?utm_campaign=Industry%20Drip&utm_medium=email&_hsenc=p2ANqtz-_8nVNDJ04OdFS2wEFSj_ztLm042deM-6uvmhTYH0z5ZWNOShaJVWGvKJQBTCKR1KGL_w-WJkmBRJbJ1IyOOwG1ixJ_KwHjPHjUd6nSg9uG3PYoIYc&_hsmi=314730085&utm_content=314730085&utm_source=hs_automation

15 Watts, C. (2024, October 23). As the U.S. election nears, Russia, Iran and China step up influence efforts. Microsoft. https://blogs.microsoft.com/on-the-issues/2024/10/23/as-the-u-s-election-nears-russia-iran-and-china-step-up-influence-efforts/

16 Thomas, E. (2024, April 1). Pro-CCP Spamouflage campaign experiments with new tactics targeting US. Institute for Strategic Dialogue. https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-campaign-experiments-with-new-tactics-targeting-the-us/

17 Thibaut, K. (2024, November 4). Trends in China's US election interference illustrate its longer game. DFRLab. https://dfrlab.org/2024/11/04/china-us-election-interference/

18 Turnnidge, S. (2024, October 17). Amazon Alexa users given false information attributed to Full Fact's fact checks. Full Fact. https://fullfact.org/online/amazon-echo-misleading-voice-assistant/

19 Jinping, X. (2019, January 25). Political Bureau of CPC Central Committee, 12th collective study session [Speech transcript]. The State Council of the People's Republic of China. https://www.gov.cn/xinwen/2019-03/15/content_5374027.htm

20 2023内容科技发展报告（简版）. (2024, April 8). 人民网研究院. http://yjy.people.com.cn/n1/2024/0408/c458741-40211694.html

21 Beauchamp-Mustafaga, N., Green, K., Marcellino, W., Lilly, S., & Smith, J. (2024). Dr. Li Bicheng, or How China Learned to Stop Worrying and Love Social Media Manipulation: Insights Into Chinese Use of Generative AI and Social Bots from the Career of a PLA Researcher. RAND. https://www.rand.org/pubs/research_reports/RRA2679-1.html

22 Tuquero, L. (2023, December 5). How generative AI could help foreign adversaries influence U.S. elections. Politifact. https://www.politifact.com/article/2023/dec/05/how-generative-ai-could-help-foreign-adversaries-i/

23 Huang, C., Silver, L., & Clancy, L. (2024, May 1). Americans Remain Critical of China. Pew Research Center. https://www.pewresearch.org/global/2024/05/01/americans-remain-critical-of-china/

24 OECD. (2024). The OECD Truth Quest Survey: Methodology and findings (Report No. 369). OECD iLibrary. https://www.oecd-ilibrary.org/docserver/92a94c0f-en.pdf?expires=1731328150&id=id&accname=guest&checksum=6FA6F3167F0A1E74366E3CC0410C674F

25 Thormundsson, B. (2024, May 14). Share of adults in the United States who were concerned about issues related to artificial intelligence (AI) as of February 2023. statistia. https://www.statista.com/statistics/1378220/us-adults-concerns-about-artificial-intelligence-related-issues/

26 Statista. (2024, September 16). Concerns among adults in the United States about the spread of political propaganda through artificial intelligence (AI) as of August 2023. https://www.statista.com/statistics/1471069/us-adults-ai-generated-political-propaganda/

27 Gottfried, J. (2020, May 28). Around three-in-ten Americans are very confident they could fact-check news about COVID-19. Pew Research Center. https://www.pewresearch.org/short-reads/2020/05/28/around-three-in-ten-americans-are-very-confident-they-could-fact-check-news-about-covid-19/

28 Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., & Saavedra, A. (2019). Students' Civic Online Reasoning: A National Portrait. Stanford History Education Group. https://stacks.stanford.edu/file/druid:gf151tb4868/Civic Online Reasoning National Portrait.pdf

29 Guess, A. M., Nyhan, B., & Reifler, J. (2020). Exposure to untrustworthy websites in the 2016 U.S. election. Nature Human Behavior, 4(5), 472-480. https://doi.org/10.1038/s41562-020-0833-x

30 Chopra, F., Haaland, I., & Roth, C. (2022). Do people demand fact-checked news? Evidence from U.S. Democrats. Journal of Public Economics, 205(1), 104549. https://doi.org/10.1016/j.jpubeco.2021.104549

31 Lyons, B., Mérola, V., Reifler, J., & Stoeckel, F. (2020). How Politics Shape Views Toward Fact-Checking: Evidence from Six European Countries. The International Journal of Press/Politics, 25(3). https://doi.org/10.1177/1940161220921732

32 Pew Research Center. (2024, June 24). Public Trust in Government: 1958-2024. https://www.pewresearch.org/politics/2024/06/24/public-trust-in-government-1958-2024/

33 United National Department of Economic and Social Affairs. (2021). Trust in public institutions: Trends and implications for economic security (Report No. 108). United Nations. https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2021/08/PB_108.pdf

34 OECD. (2023). Trust in government. https://www.oecd.org/en/data/indicators/trust-in-government.html?oecdcontrol-3122613a85-var3=2023

35 Meta. (2023, January 30). Restricting accounts of public figures during civil unrest. https://transparency.meta.com/en-gb/enforcement/taking-action/restricting-accounts-by-public-figures/

36 Oversight Board. (2021, May 5). Oversight Board Upholds Former President Trump's Suspension, Finds Facebook Failed to Impose Proper Penalty. https://www.oversightboard.com/news/226612455899839-oversight-board-upholds-former-president-trump-s-suspension-finds-facebook-failed-to-impose-proper-penalty/

37 Clegg, N. (2023, January 25). Ending Suspension of Trump's Accounts With New Guardrails to Deter Repeat Offenses. Meta. https://about.fb.com/news/2023/01/trump-facebook-instagram-account-suspension/

38 https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/

39 Lyons, J. (2023, February 11). Let's play a game: Deepfake news anchor or real person?. The Register. https://www.theregister.com/2023/02/11/deepfake_news_anchors/

40 Microsoft Threat Intelligence. (2024, April 4). Same targets, new playbooks: East Asia threat actors employ unique methods. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/east-asia-threat-actors-employ-unique-methods#section-master-oc526b

41 OpenAI. (2024, February 14). Disrupting malicious uses of AI by state-affiliated treat actors. https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/

42 https://deepmind.google/technologies/veo/veo-2/

43 OpenAI. (n.d.). Sora. https://sora.com/

44 From Babbage from The Economist: Gary Marcus: a sceptical take on AI in 2025, 15 Jan 2025 https://podcasts.apple.com/gb/podcast/babbage-from-the-economist/id508376907?i=1000684121035&r=1920

45 Keast, J. (2023). Shadow Play: A pro-China technology and anti-US influence operation thrives on YouTube (Report No. 77). Australian Strategic Policy Institute. https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-12/Shadow%20Play.pdf?VersionId=1_.62RpM_chdUdpm7I0da34yOfAvR0t6

46 Spring, M. (2024, October 5). The racist AI deepfake that fooled and divided a community. BBC. https://www.bbc.co.uk/news/articles/ckg9k5dvlzdo

47 Export Compliance Training Institute. (2022, December 20). Understanding the Foreign Direct Product Rule. https://www.learnexportcompliance.com/understanding-the-foreign-direct-product-rule/

48 Bureau of Industry and Security. (2024, December 2). Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications [Press Release]. https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced

49 Morrison Foerster. (2024, March 14). UK Expands Export Controls to Semiconductor and Other Emerging Technologies. https://www.mofo.com/resources/insights/240314-uk-expands-export-controls-to-semiconductor

50 Pan, C. (2024, September 16). China hit hard by new Dutch export controls on ASML chip-making equipment. South China Morning Post. https://www.scmp.com/tech/tech-war/article/3278535/china-hit-hard-new-dutch-export-controls-asml-chip-making-equipment

51 Perozo, E. (2024, September 2). China threatens to retaliate after Japan imposes export regulations. Investment Monitor. https://www.investmentmonitor.ai/news/china-threatens-to-retaliate-after-japan-imposes-export-regulations/

52 Benaich, N., & Air Street Capital. (2024). State of AI Report 2024 (Report No. 7). https://www.stateof.ai/

53 Benaich, N., & Air Street Capital. (2024). State of AI Report 2024 (Report No. 7). https://www.stateof.ai/

54 Benaich, N., & Air Street Capital. (2024). State of AI Report 2024 (Report No. 7). https://www.stateof.ai/

55 Sherman, N. (2024, December 11). Nvidia targeted by China in new chip war probe. BBC. https://www.bbc.co.uk/news/articles/cx2vkd90mk8o

56 https://www.bbc.co.uk/news/articles/c5yv5976z9po

57 Benaich, N., & Air Street Capital. (2024). State of AI Report 2024 (Report No. 7). https://www.stateof.ai/

58 Exec. Order No. 14,110, 3 C.F.R. 75191-75226 (2023). https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

59 Republican Party. (2024, July 8). 2024 GOP Platform Make America Great Again!, 9. https://prod-static.gop.com/media/RNC2024-Platform.pdf?_gl=1*lkwqi4o*_gcl_au*MjMzMjk5Mzc5LjE3MzMzNjQ1ODI.&_ga=2.79801364.2029520348.1734397581-53960822.1733364582

60 https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

61 https://youtu.be/64E9O1Gv99o?t=68

62 Clegg, N. (2024, February 6). Labeling AI-Generated Images on Facebook, Instagram and Threads. Meta. https://about.fb.com/news/2024/02/labeling-ai-generated-images-on-facebook-instagram-and-threads/

63 Meta. (2024, April 2). How fact-checking works. https://transparency.meta.com/en-gb/features/how-fact-checking-works/

64 Coalition for Content Provenance and Authenticity. (n.d.). Overview. https://c2pa.org/

65 Google DeepMind. (n.d.). SynthID. https://deepmind.google/technologies/synthid/

66 Dathathri, S., See, A., Ghaisas, S., Huang, P., McAdam, R., Welbl, J., Bachani, V., Kaskosoli, A., Stanforth, R., Matejovicova, T., Hayes, J., Vyas, N., Merey, M. A., Bowen-Cohen, J., Bunel, R., Balle, B., Cemgil, T., Ahmed, Z., Stacpoole, K., ...Kohli, P. (2024). Scalable watermarking for identifying large language model outputs. Nature, 634(1), 818-823. https://www.nature.com/articles/s41586-024-08025-4

67 AFP Fact Check. (n.d.). US Elections 2024. https://factcheck.afp.com/list/US-elections-2024

68 Jiang, B. (2024, April 13). More than 600 million on mainland now use LLMs amid rapid growth in GenAI adoption: report. South China Morning Post. https://www.scmp.com/tech/tech-trends/article/3274328/more-600-million-mainland-now-use-llms-amid-rapid-growth-genai-adoption-report

69 European Commission. (2024, August 16). Commission sends request for information to Meta under the Digital Services Act [Press Release]. https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-2

70 Wakefield, J. (2020, June 5). How Bill Gates became the voodoo doll of Covid conspiracies. BBC. https://www.bbc.co.uk/news/technology-52833706

71 Neville, M. (Writer & Director). (2024, September 18). Truth or Consequences? (Season 1, Episode 2) [TV series episode]. In Marson, E., & Roger, C. (Executive Producers), What's Next: The Future with Bill Gates. Netflix. https://www.netflix.com/watch/81680795.

72 Bannister, K. (2018, February 26). Understanding Sentiment Analysis: What It Is & Why It's Used. Brandwatch. https://www.brandwatch.com/blog/understanding-sentiment-analysis/

73 SimPPL. Research. (n.d.). https://simppl.org/research

74 Prototypes for Humanity. (n.d.). #2024 Is That True?. https://www.prototypesforhumanity.com/project/is-that-true/

75 Deeplake. (n.d.). LIAR Dataset. https://datasets.activeloop.ai/docs/ml/datasets/liar-dataset/#:~:text=LIAR%20Dataset%2C%20is%20a%20new,%2C%20party%2C%20and%20past%20date.

76 Federal Trade Commission. (2024). OriginStory: Authenticating the human origin of voice at the time of recording. https://www.ftc.gov/system/files/ftc_gov/pdf/OriginStory-Abstract.pdf

77 See Invisible Rulers: The People Who Turn Lies into Reality.

78 Federal Trade Commission. (2024). OriginStory: Authenticating the human origin of voice at the time of recording. https://www.ftc.gov/system/files/ftc_gov/pdf/OriginStory-Abstract.pdf

79 Regulation (EU) 2022/2065. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) https://www.eu-digital-services-act.com/Digital_Services_Act_Article_69.html

80 Goujard, C., & Volpicelli, G. (2024, May 16). EU hits Meta with new probe over 'addictive' algorithms harming children. Politico. https://www.politico.eu/article/meta-hit-with-new-eu-probe-over-addictive-algorithms-harming-children/

81 Poritz, I. (2024, October 24). Meta, Google, TikTok Must Face Schools' Addiction Claims. Bloomberg. https://www.bloomberg.com/news/articles/2024-10-24/social-media-giants-must-face-school-districts-addiction-claims

82 New York State Attorney General. (2024, March 14). Attorney General James Champions Legislation to Protect Kids from Addictive Social Media Feeds in National USA Today Op-Ed [Press Release]. https://ag.ny.gov/press-release/2024/attorney-general-james-champions-legislation-protect-kids-addictive-social-media

83 Howard, P. N., & Hussain, M. M. (2013). Digital Media and the Arab Spring. In Howard, P. N., & Hussain, M. M. (Eds.), Democracy's Fourth Wave? Digital Media and the Arab Spring (pp. 17-34). Oxford Studies in Digital Politics. https://ora.ox.ac.uk/objects/uuid:05e13455-3e16-478b-b0b3-f75b58ef489c/files/m047d301ca586576dc9ba2eea1833lee0

84 Smidi, A., & Shahin, S. (2017). Social Media and Social Mobilisation in the Middle East: A Survey of Research on the Arab Spring. India Quarterly, 73(2), 196-209. https://www.jstor.org/stable/48505308

85 Schiffrin, A. (2017). Disinformation and Democracy: The internet transformed protest but did not improve democracy. Journal of International Affairs, 71(1), 117-126. https://www.jstor.org/stable/26494367

86 Kurlantzick, J. (2020, September 10). How China Ramped Up Disinformation Efforts During the Pandemic. Council on Foreign Relations. https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic

87 Wendler, J. R. (2021). Misleading a Pandemic: The Viral Effects of Chinese Propaganda and the Coronavirus. Joint Force Quarterly, 104(1). https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2884217/misleading-a-pandemic-the-viral-effects-of-chinese-propaganda-and-the-coronavir/

88 Kinetz, E. (2021, February 15). Anatomy of a conspiracy: With COVID, China took leading role. AP News. https://apnews.com/article/pandemics-beijing-only-on-ap-epidemics-media-122b73e134b780919cc1808f3f6f16e8

89 Ibid

90 Coldewey, D. (2024, May 30). Misinformation works, and a handful of social 'supersharers' sent 80% of it in 2020. TechCrunch. https://techcrunch.com/2024/05/30/misinformation-works-and-a-handful-of-social-supersharers-sent-80-of-it-in-2020/

91 World Health Organization. (2021, April 27). Fighting misinformation in the time of COVID-19, one click at a time. https://www.who.int/news-room/feature-stories/detail/fighting-misinformation-in-the-time-of-covid-19-one-click-at-a-time

92 Caceres, M. M. F., Sosa, J. P., Lawrence, J. A., Sestacovschi, C., Tidd-Johnson, A., Rasool, M. H. U., Gadamidi, V. K., Ozair, S., Pandav, K., Cuevas-Lou, C., Parrish, M., Rodriguez, I., & Fernandez, J. P. (2022). The impact of misinformation on the COVID-19 pandemic. AIMS Public Health, 9(2), 262-277. https://doi.org/10.3934/publichealth.2022018

93 Schaeffer, K. (2020, July 24). A look at the Americans who believe there is some truth to the conspiracy theory that COVID-19 was planned. Pew Research Center. https://www.pewresearch.org/short-reads/2020/07/24/a-look-at-the-americans-who-believe-there-is-some-truth-to-the-conspiracy-theory-that-covid-19-was-planned/

94 Uscinski, J. E., Enders, A. M., Klofstad, C., Seelig, M., Funchion, J., Everett, C., Wuchty, S., Premaratne, K., & Murthi, M. (2020). Why do people believe COVID-19 conspiracy theories?. Harvard Kennedy School (HKS) Misinformation Review. https://doi.org/10.37016/mr-2020-015

95 Nimmo, B., Hubert, I., & Cheng, Y. (2021). Spamouflage Breakout. Graphika. https://graphika.com/reports/spamouflage-breakout

96 Nimmo, B., Hubert, I., & Cheng, Y. (2021). Spamouflage Breakout. Graphika. https://graphika.com/reports/spamouflage-breakout

97 Hundreds of fake Twitter accounts linked to China sowed disinformation prior to the US election – report. (2021, January 28). Cardiff University News. https://www.cardiff.ac.uk/news/view/2491763-hundreds-of-fake-twitter-accounts-linked-to-china-sowed-disinformation-prior-to-the-us-election,-with-some-continuing-to-amplify-reactions-to-the-capitol-building-riot-report

98 Rogin, J. (2020, October 29). There's Chinese interference on both sides of the 2020 election. The Washington Post. https://www.washingtonpost.com/opinions/global-opinions/theres-chinese-interference-on-both-sides-of-the-2020-election/2020/10/29/49f90dfe-1a2c-11eb-82db-60b15c874105_story.html

99 Eisenman, J., & Grizzell, H. (2021, March 24). Beijing's Schadenfreude Over the Capitol Riots Conceals Deep Anxiety. Foreign Policy. https://foreignpolicy.com/2021/03/24/beijing-capitol-riot-elections-xi-jinping/

100 Graphika. (2024). The #Americans. https://graphika.com/reports/the-americans

101 National Intelligence Council. (2021). Foreign Threats to the 2020 US Federal Elections (Report No. ICA 2020-00078D). https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

102 Graphika. (2024). The #Americans. https://graphika.com/reports/the-americans

103 Watts, C. (2024, April 4). China tests US voter fault lines and ramps AI content to boost its geopolitical interests. Microsoft. https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/

104 Cybersecurity & Infrastructure Security Agency. (2018, May). Social Media Bots Overview. https://www.cisa.gov/sites/default/files/publications/19_0717_cisa_social-media-bots-overview.pdf

105 Bowden, J. (2024, October 9). 2024 election to be most expensive in history with $15.8bn spent, new report reveals. Independent. https://www.independent.co.uk/news/world/americas/us-politics/2024-trump-harris-election-spending-b2626617.html

106 Watts, C. (2023, September 7). China, North Korea pursue new targets while honing cyber capabilities. Microsoft. https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/

107 U.S. Department of Justice. (2024, September 4). Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere [Press Release]. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

108 Simon, S. (2024, September 7). DOJ says Russia paid right-wing influencers to spread Russian propaganda. NPR. https://www.npr.org/2024/09/07/nx-s1-5101895/doj-says-russia-paid-right-wing-influencers-to-spread-russian-propaganda

109 Bing, C., & Paul, K. (2024, September 3). US voters targeted by Chinese influence online, researchers say. Reuters. https://www.reuters.com/world/us/us-voters-targeted-by-chinese-influence-online-researchers-say-2024-09-03/

110 ABC News. (2024, August 29). New study alleges Chinese government is using TikTok to influence U.S. users [Video]. YouTube. https://www.youtube.com/watch?v=rsZyF5efQek

111 Embassy of the People's Republic of China in the United Kingdom of Great Britain and Northern Ireland. (2023, September 14). Embassy Spokesperson on the UK Government's response to the Intelligence and Security Committee of Parliament report 'China'. http://gb.china-embassy.gov.cn/eng/PressandMedia/Spokepersons/202309/t20230915_11143290.htm

112 Zhang, L. (2020, March 2). FALQs: Spreading Rumors and Police Reprimand Under Chinese Law. Library of Congress Blogs. https://blogs.loc.gov/law/2020/03/falqs-spreading-rumors-and-police-reprimand-under-chinese-law/

113 In China, fib online and find out. (2024, October 17). The Economist. https://www.economist.com/china/2024/10/17/in-china-fib-online-and-find-out

114 Text - H.R.815 - 118th Congress (2023-2024): Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes. (2024, April 24). https://www.congress.gov/bill/118th-congress/house-bill/815/text

115 The Economic Times. (2024, February 2). TikTok CEO denies links with Communist Party of China, says "I'm Singaporean!" | US Senate Hearing [Video]. YouTube. https://www.youtube.com/watch?v=EVDsImdq4Yg

116 TikTok Inc. v. Merrick Garland, 24-1113, (D.C. Cir. 2024). https://www.courtlistener.com/docket/68506893/01208647195/tiktok-inc-v-merrick-garland/

117 Allyn, B. (2024, August 15). TikTok fights for survival in latest filing as ban approaches. NPR. https://www.npr.org/2024/08/15/nx-s1-5077782/tiktok-survival-filing-ban-approaches

118 ABC News. (2024, August 29). New study alleges Chinese government is using TikTok to influence U.S. users [Video]. YouTube. https://www.youtube.com/watch?v=rsZyF5efQek

119 TikTok Inc. v. Merrick Garland, 24-1113, (D.C. Cir. 2024). https://www.courtlistener.com/docket/68506893/01208647195/tiktok-inc-v-merrick-garland/

120 TikTok Inc. v. Merrick Garland, 24-1113, (D.C. Cir. 2024). https://www.courtlistener.com/docket/68506893/01208647195/tiktok-inc-v-merrick-garland/

121 TikTok Inc. v. Merrick Garland, 24-1113, (D.C. Cir. 2024). https://www.courtlistener.com/docket/68506893/01208647195/tiktok-inc-v-merrick-garland/

122 TikTok Inc. v. Merrick Garland, 24-1113, (D.C. Cir. 2024). https://www.courtlistener.com/docket/68506893/01208647195/tiktok-inc-v-merrick-garland/

123 Maza, C. (2018, September 19). Why These Chinese Media Companies Have to Register As Foreign Agents. Newsweek. https://www.newsweek.com/why-these-chinese-media-companies-have-register-foreign-agents-1128649

124 According to the DoJ's website, a "foreign principal" and be: "a foreign government, a foreign political party, any person outside the United States (except U.S. citizens who are domiciled within the United States), and any entity organized under the laws of a foreign country or having its principal place of business in a foreign country. It can also include a foreign faction or body of insurgents whose legitimacy the United States government has yet to recognize. U.S. Department of Justice. (n.d.). Foreign Agents Registration Act – Frequently Asked Questions. https://www.justice.gov/nsd-fara/frequently-asked-questions

125 United States Department of Justice. (n.d.). Foreign Agents Registration Act – Browse Filings. https://efile.fara.gov/ords/fara/f?p=1381:1:5042331505515

126 Registering under FARA is not groundbreaking in itself, many organisations from allied countries - from the UK's British Tourist Authority, to Australia's New South Wales Government - are signed up. What was noticeable was the timing and the fact that these were specifically news companies. The DOJ's China decision puts Beijing on a par with Moscow, as in November 2017 two Russian outlets were given the same treatment.

127 United States Department of Justice. (n.d.). Foreign Agents Registration Act – Browse Filings. https://efile.fara.gov/ords/fara/f?p=1381:1:5042331505515

128 FARA requires agents to provide public awareness of their activities to influence public opinion and policies in the US, maintain significant records of their work, and ensure they are transparent about materials they share.

U.S. Department of Justice. (n.d.). Foreign Agents Registration Act – Frequently Asked Questions. https://www.justice.gov/nsd-fara/frequently-asked-questions

129 Microsoft. (2024, April 4). China tests US voter fault lines and ramps AI content to boost its geopolitical interests. https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/

130 Foreign Agents Registration Act of 1928, 22 U.S.C. § 11 (2009). https://www.govinfo.gov/content/pkg/USCODE-2009-title22/pdf/USCODE-2009-title22-chap11-subchapII.pdf

131 U.S. Department of Justice. (2024, September 3). Former High-Ranking New York State Government Employee Charged with acting as an Undisclosed Agent of the People's Republic of China and the Chinese Communist Party [Press Release]. https://www.justice.gov/opa/pr/former-high-ranking-new-york-state-government-employee-charged-acting-undisclosed-agent

132 U.S. Department of Justice. (2024, September 4). Two RT employees Indicted for Covertly Funding and Directing U.S. Company that Published Thousands of Videos in Furtherance of Russian Interests [Press Release]. https://www.justice.gov/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands

133 U.S. Department of the Treasury. (2024, September 4). Treasury Takes Action as Part of a U.S. Government Response to Russia's Foreign Malign Influence Operations [Press Release]. https://home.treasury.gov/news/press-releases/jy2559

134 U.S. Department of Justice. (2024, September 4). Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operations Targeting Audiences in the United States and Elsewhere [Press Release]. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

135 U.S. Department of Justice. (2018, February 16). Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System [Press Release]. https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere

136 Dilanian, K., Williams, P., & Winter, T. (2020, March 17). Why did the Justice Department drop its prosecution of 2 firms linked to a Putin associate?. NBC News. https://www.nbcnews.com/politics/justice-department/why-did-justice-department-drop-its-prosecution-2-firms-linked-n1161886

137 U.S. Department of Justice. (2024, September 18). Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers [Press Release]. https://www.justice.gov/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

138 U.S. Department of Justice. (2024, August 23). Florida Telecommunications and Information Technology Worker Pleads Guilty to Conspiring to Act as Agent of PRC Government [Press Release]. https://www.justice.gov/opa/pr/florida-telecommunications-and-information-technology-worker-pleads-guilty-conspiring-act

139 According to the DoJ's website, the definition of an "agent of a foreign principal" is: "someone who acts as an agent, representative, employee, or servant, or otherwise acts at the order, request, or under the direction or control of a "foreign principal"" See: https://www.justice.gov/nsd-fara/frequently-asked-questions U.S. Department of Justice. (n.d.). Foreign Agents Registration Act – Frequently Asked Questions. https://www.justice.gov/nsd-fara/frequently-asked-questions

140 Kelner, R. K., Smith, B. D., & Langton, K. (2023, May 31). DOJ Releases New FARA Advisory Opinions Affecting Digital Media Platforms. Lexology. https://www.lexology.com/library/detail.aspx?g=f8213304-a9dc-4e0d-9ae9-0b39e03f3b0b

141 Hickey, A. S., Keeler, T. J., Becker, J. H., Leibner, M., & Shah, R. (2024, January 12). The US Foreign Agents Registration Act (FARA): Key Issues to Watch in 2024. Mayer|Brown. https://www.mayerbrown.com/en/insights/publications/2024/01/the-us-foreign-agents-registration-act-fara-key-issues-to-watch-in-2024

142 https://www.justice.gov/ag/media/1388541/dl

143 Murthy v. Missouri, 23-411. 2 (U.S. Sup. Ct. 2023). https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf

144 https://www.youtube.com/watch?v=XPZAtf3VRWI&t=175s

145 https://www.justice.gov/ag/media/1388541/dl

146 Murthy v. Missouri, 23-411. 9 (U.S. Sup. Ct. 2023). https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf

147 Murthy v. Missouri, 23-411. 28 (U.S. Sup. Ct. 2023). https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf

148 Murthy v. Missouri, 23-411. 5-6 (U.S. Sup. Ct. 2023). https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf

149 Murthy v. Missouri, 23-411. 5 (U.S. Sup. Ct. 2023). https://www.supremecourt.gov/opinions/23pdf/23-411_3dq3.pdf

150 Watson, A. (2023, August 16). Public opinion on government restricting false news online in the United States from 2018 to 2023. Statista. https://www.statista.com/statistics/829242/government-intervention-fake-news/

151 Watson, A. (2023, August 16). Public opinion on tech companies restricting false news online in the United States in 2018 and 2023. Statista. https://www.statista.com/statistics/829260/tech-company-intervention-fake-news/

152 U.S. Department of Justice. (2024, September 4). Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere [Press Release]. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

153 Center for Internet Security. (n.d.). Reporting Misinformation to the EI-ISAC. https://www.eac.gov/sites/default/files/partners/EI_ISAC_Reporting_Misinformation_Sheet102820.pdf

154 United Kingdom Cabinet Office. (2023, June 9). Fact Sheet on the CDU and RRU. https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru

155 Secrétariat général de la défense et de la sécurité nationale. (n.d.). Une organisation au cœur de l'exécutif. https://www.sgdsn.gouv.fr/

156 Australian Electoral Commission. (2024, April 17). Disinformation register. https://www.aec.gov.au/media/disinformation-register.htm

157 Oversight Board. (n.d.). Case Decision and Policy Advisory Opinions. https://www.oversightboard.com/decision/

158 Oversights Board. (n.d.). Tracking the Implementation of Our Recommendations. https://www.oversightboard.com/recommendation-tracker/

159 Edwards-Levy, A. (2024, September 11). CNN Flash Poll: Majority of debate watchers say Harris outperformed Trump onstage. CNN. https://edition.cnn.com/2024/09/11/politics/election-poll-trump-harris-debate/index.html

160 https://www.reuters.com/fact-check/zelenskiys-latest-approval-rating-is-63-not-4-contrary-trumps-claim-2025-02-21/

161 https://www.politifact.com/factchecks/2024/may/15/joe-biden/joe-biden-wrong-that-he-inherited-9-inflatio/

162 https://www.bbc.co.uk/news/articles/cgjv3gdxv7go

163 Centers for Disease Control. (n.d.). Tips From Former Smokers. https://www.cdc.gov/tobacco/campaign/tips/index.html

164 U.S. Department of Health and Human Services. (n.d.). Risk Less. Do More. https://www.hhs.gov/risk-less-do-more/index.html

165 National Highway Traffic Safety Administration. (n.d.). Seat Belts Save Lives. https://www.nhtsa.gov/campaign/click-it-or-ticket

166 U.S. Department of Agriculture. (n.d.). Learn how to eat healthy with MyPlate. https://www.myplate.gov/

167 It's On Us. (n.d.). Home. https://itsonus.org/

168 Partnership to End Addiction. (n.d.). Home. https://drugfree.org/

169 Cybersecurity & Infrastructure Security Agency. (n.d.). Election Security Rumor vs. Reality. https://www.cisa.gov/topics/election-security/rumor-vs-reality

170 Cybersecurity & Infrastructure Security Agency. (2024, September 12). Just So You Know: False Claims of Hacked Voter Information Likely Intended to Sow Distrust of U.S. Elections [Public Service Announcement]. https://www.cisa.gov/sites/default/files/2024-09/PSA_Just_So_You_Know_False_Claims_of_Hacking_Voter_Reg_CISA_and_FBI-508_0.pdf

171 Coldewey, D. (2024, May 30). Misinformation works, and a handful of social 'supersharers' sent 80% of it in 2020. TechCrunch. https://techcrunch.com/2024/05/30/misinformation-works-and-a-handful-of-social-supersharers-sent-80-of-it-in-2020/

172 Ivan, C., Chiru, I., Buluc, R., Radu, A. Anghel, A., Stoian-Iordache, V. Arcos, R., Arribas, C. M., Ćuća, A., Ganatra, K., Gertrudix, M., Modh,K., & Nastasiu, C. (2023). HANDBOOK on Identifying and Countering Disinformation. DOMINOES Project. https://doi.org/10.5281/zenodo.7893952

173 Maertens, R., Roozenbeek, J., Basol, M., & van der Linden, S. (2021). Long-term effectiveness of inoculation against misinformation: Three longitudinal experiments. Journal of Experimental Psychology: Applied, 27(1), 1–16. https://doi.org/10.1037/xap0000315

174 https://pubmed.ncbi.nlm.nih.gov/33017160/

175 Ibid

176 Lewsey, F. (n.d.). Cambridge game 'pre-bunks' coronavirus conspiracies. University of Cambridge. https://www.cam.ac.uk/stories/goviral

177 Graber, J. (2023, May 30). Algorithmic choice. Bluesky. https://bsky.social/about/blog/3-30-2023-algorithmic-choice

178 Office of Governor Gavin Newsom, (2024, September 17). Governor Newsom signs bill to combat deepfake election content [Press Release]. https://www.gov.ca.gov/2024/09/17/governor-newsom-signs-bills-to-combat-deepfake-election-content

179 Texas Economic Development & Tourism. (n.d.). Texas Enterprise Fund. https://gov.texas.gov/business/page/texas-enterprise-fund

180 National Science Foundation. (n.d.). America's Seed Fund. https://seedfund.nsf.gov/

181 U.S. White House. (2023, July). Voluntary AI Commitments. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

182 Mislove, A. (2023, August 29). Red-Teaming Large Language Models to Identify Novel AI Risks. United States Office of Science and Technology Policy https://bidenwhitehouse.archives.gov/ostp/news-updates/2023/08/29/red-teaming-large-language-models-to-identify-novel-ai-risks/

A visitor toasts with an ancient poet at the World Internet Conference Wuzhen Summit on Nov. 21, 2024, in Wuzhen, China. (Wang Gang / China News Service / VCG via Getty Images)

Culture as a Tool for Trustworthy AI

Averill Campion

Introduction

The current logic of trustworthy AI is that the combination of top-down AI principles and centralized regulatory efforts will control AI actors' behavior. This logic entails that AI actors should incorporate AI principles throughout the AI lifecycle and respond to regulations. As a result, the theory is that society will widely adopt AI because it accepts a degree of vulnerability based on positive expectations[1] about the intention and behavior of AI actors, the AI applications they use, and government's ability to protect them from harm.

This important formula is still limited because it does not capture the full picture of how trust is institutionalized. The trustworthy AI formula can benefit from also leveraging cultural-cognitive and normative elements, in addition to the regulative elements that tend to be more top-down and coercive in nature. Cultural-cognitive mechanisms are a crucial but often-overlooked tool for how values are translated into prescriptions about the appropriate way to do something, which tends to be dependent on local context. It is now a national security priority for the U.S. and its allies to build "technology for freedom or watch as others build for control."[2]

Therefore, the aim of this policy report is twofold: First, it intends to illuminate how cultural-cognitive elements can play a role in supporting AI development with democratic values; second, it intends to convey why policy makers should ensure the structural provisions are in place for bottom-up initiatives such as partnerships across research labs, civil society, grassroots organizations, and the multitude collaborative efforts that provide the face-to-face interaction necessary for creating shared conceptions and meaning about AI governance. By helping policymakers better understand how culture is a tool for trustworthy AI development, this report both responds to calls for ensuring that the global majority possesses agency in determining their AI governance future while also illuminating the paths that counter techno-authoritarian values.

Decisions about prescriptive, evaluative, and obligatory aspects of behavior often combine or interact with cultural elements to the form practices, standards, roles, conventions, and codes[3] needed to institutionalize AI governance. Cultural-cognitive mechanisms are the mental models or "operating mechanisms of the mind" that shape the share beliefs, categories, heuristics, and logics of actions.[4] This is a relational process that often requires spontaneous human interaction to occur. Just like the seemingly invisible algorithms that people use to make decisions daily,[5] establishing a combination of regulatory, normative, and cognitive-cultural mechanisms for AI development will create the often unseen but stable infrastructure upon which society builds its shared meaning and positive expectations[6] about AI.

The Institutional Toolbox: Trustworthy AI

Trust building is a long-term process based on characteristics like competency, benevolence, and integrity. It is hard to disassociate the human from trustworthy AI, even if widespread AI adoption refers to the ability to trust the technology (or application) itself. Therefore, it is imperative that the foundations upon which these tools and applications are being developed support human flourishing and set up the means for humans to interact around collaborative AI development. An effective way to shape value systems in organizations is through cultural-cognitive and normative mechanisms.

Establishing the right sort of trust pattern needs more illumination. Trust patterns can be established over time from repeated interactions, but just because those trust patterns have been established doesn't mean they are infused with the appropriate guidelines of what is important enough to prevent violations of that trust. Trust based purely on another party's competency might be good enough to create a long-term commitment, but is it enough to assess whether the competent, trusted party will not attempt to cause future harm? With regard to national security and the promotion of technology based on democratic values, the U.S. and its allies must be vigilant and look beyond the regulations enacted to support global principles like "AI for the public good" and further analyze the underlying norms and culture that guide the interpretation of these principles. Moreover, the U.S. must be proactive in setting up collaborative efforts and partnerships that will create cultures conducive to democratic value interpretations. An important indicator about whether techno-authoritarianism is a model to be exported can be examined by the way actors specify how things should be accomplished in partnerships and other types of interorganizational collaboration for technology.

AI for the Public Good and Responsible AI

While principles are unquestionable meanings, principles are interpreted through different combinations of values. Therefore, it makes sense that global-seeming principles such as "AI for the public good" contain different meanings throughout the world. At the global level, themes like "AI for the public good/public interest," "responsible AI," and "AI safety" are being prioritized. For example, responsible AI is being implemented through networks like the Partnership on AI, whose mission is to bring together diverse voices so developments in AI advance positive outcomes for people and society, while AI for the public interest was a major theme at the 2025 AI Action Summit in Paris. By unraveling the normative background of trust building, it can be better deciphered how shared concepts influence the social reality.

A global effort to set up a shared meaning about AI governance must also be considered alongside the fact that nations have a degree of self-interest in

institutionalizing their own norms into these principles. China is also embracing the principle that AI should be for the public good. The Ministry of Foreign Affairs for the People's Republic of China announced in September 2024 an "AI Capacity-Building Action Plan for Good and for All"[7] that calls for the establishment of an international cooperation platform to promote AI capacity-building, programs in developing countries to enhance education and exchanges, and global, interoperable AI risk assessment frameworks and standards.

It is unclear how intentional China's efforts may be to infuse its own normative and regulatory values abroad. There are some suggestions that China is promoting surveillance technology and cyberspace governance norms through Chinese "training sessions and seminars with over thirty countries on cyberspace and information policy," and invitations to journalists and media to learn about "socialist journalism with Chinese characteristics."[8] Furthermore, AI safety is a concern shared by Chinese policymakers, as evidenced through increases of this topic in research papers, public statements, and government documents.[9]

In the Western context, democratic values must be safeguarded to ensure the internet upholds its commitment to decentralized networks and freedom in contrast to authoritarian regimes, as seen through initiatives like the international partnership surrounding the Declaration for the Future of the Internet.[10] Distinguishing visions is important because the Western interpretation of AI for the public good, especially in the U.S., can often mean protecting human rights and freedoms, as opposed to other national contexts where it could mean putting the collective above the individual, especially when individuality threatens stability of the collective in times of uncertainty. In democracies, AI (assisted) decisions about the common good are *not* indisputable, even in the name of the public interest. Boundaries about when the collective good does or does not override the individual good must be drawn just as the Founding Fathers institutionalized for Americans.

Regulatory Elements as a Tool for Trustworthy AI

The point of a regulatory tool as an institutional mechanism is to set rules, monitor, and sanction when conformity is violated.[11] The U.S. has not taken a federal-level approach to regulating AI, and the fragmentation across state-level laws is making it difficult for platforms to navigate.[12] Thirty-four out of 50 states have proposed some form of AI legislation.[13]

A teacher trains students on how to use DeepSeek and other AI tools at a night school in Hangzhou, China, on March 12, 2025. (Jiang Zitong / Zhejiang Daily Press Group / VCG via Getty Images)

While regulation is not the focus of this report, it is important to note even authoritarian regimes implement cyber and data privacy protections. There are even mirrored intentions between China's Personal Information Protection Law and the EU's GDPR regulation of protecting personal information.[14] However, authoritarian privacy is the idea that autocracies are proponents of privacy law, repressing citizens but protecting their privacy as a form of legitimizing and maintaining the surveillance state.[15] China, for example, is proactive in information privacy law and enforcement to portray itself as a "benevolent guardian" against "intruders."[16]

China has also built an "extensive governance regime for cyberspace and information and communications technology (ICT)" with policy "spanning cybersecurity, the digital economy, and online media content – all under one mantel" that provide rules for data protection, crucial infrastructure, encryption, internet content and so forth.[17] Policymakers must pay attention to how new rules for AI governance are shaped because Chinese think tanks and scholars are also pursuing the Chinese Communist Party's version of solutions abroad for things like global cloud governance and the idea of data sovereignty and data localization.[18] One important characteristic of techno-authoritarianism from the Chinese model is that Chinese companies, even when abroad, are compelled by law to install "backdoors in equipment or software."[19]

It is beyond the scope of this report to examine in detail the extant differences and similarities between varieties of AI regulation since research exists on the intricate distinctions.[20] Instead, this provides an overview to encourage continued discussion on the topic of regulation for subjects like data privacy. Overall, regulation as a tool for institutionalizing trust should not be completely taken off the table, especially as a coordination mechanism to unify state efforts. The U.S. doesn't have to copy the EU's GDPR law but could instead ask what we have learned since the passing of GDPR, what could be improved upon, and what could be done differently to set a baseline of data protection for citizens, for example. Topics like data privacy remain relevant, considering that DeepSeek emerged as an innovative foundational model despite regulatory considerations in China.

Normative Elements as a Tool for Trustworthy AI

Norms are the second mechanisms in the institutional toolbox and are defined as the "standards, roles, conventions, practices, customs and the codes of conduct that guide behavior."[21] Norms often contribute to behavior shaping much faster than regulation. Mark Zuckerberg's recent statement[22] about internal changes being made at Meta with regard to content moderation exemplifies the speed at which the implementation of practices and processes internal to an organization can change the prescriptions around how a value like free speech is interfaced to billions of users worldwide. Moreover, Meta illustrates that company self-monitoring and the structural change of international policies and processes from both a technical and non-technical standpoint occur quickly when pressure is in place. This example represents how nonstate actors possess the ability to both rapidly respond to changes and adapt the way their algorithms interact with humans, showing speed, flexibility, and agility.

Cultural-Cognitive Elements as a Tool for Trustworthy AI

Culture-cognitive elements sit at the bottom of collaborations across sectors, partnerships, networks, and organizations in general. These tools may be softer than normative and regulatory elements,[23] but cultivating this ethos and spirit provides a much deeper and more fundamental dimension related to beliefs and meaning. Collaborators must attempt to bridge a shared meaning across multiple logics, with each logic containing belief systems, different aims, and strategies for obtaining those aims.[24] Mark Andreessen, the co-author of Mosaic and co-founder of Netscape, stated[25] that this sort of intangible spirit is always there and keeps bouncing back. A Financial Times article describes how at Davos 2025, EU leaders were said to be alarmed and in an existential crisis, with other references to the "increase in animal spirits" in corporate sentiment.[26]

In terms of policy, the idea is to set up the structure or enable structural elements to be in place to allow a culture and ethos based on democratic values to flourish. We see this happening on the venture capital scene with Ex/Ante, a fund backed by Eric Schmidt

that focuses on agentic tech based on "technology that works to support human agency through things like individual control over things like your privacy."[27] The most effective way is structuring culture to emerge through collaborative organizational forms and initiatives that create a diverse pool of ideas and information and that can provide insight into local contextual needs and concerns.

Beyond Rock, Paper, Scissors

A rock-paper-scissors game among national security, economic competition, and the innovation-risk tension over AI development is prevalent. From the lens of great AI power competition, the United States' and China's tech leadership is evident both domestically and internationally. Both countries are at the forefront of capability in providing a suite of AI packages to governments including offers in telecom infrastructure[28] like 5G mobile networks, fiber optic cables, and satellites, fintech, and smart cities; data infrastructure like data centers, and cloud computing services; open- and closed-source foundational models; and AI applications and tools.

U.S efforts to curtail China's increasing capabilities are underway with export controls on AI chips and restrictions on outbound investments that can widen the gap between these two competitors, alongside new efforts to carefully manage security threats to intellectual property.[29]

Economic Competition Doesn't Counter Innovation or Agency

The opportunity to pursue innovative solutions using AI that create benefits for society is not limited by economic competition or the fact that two states tend to control the "AI triad of inputs:" compute, data, and algorithms.[30] First, as shown by the release of DeepSeek R1, AI companies in different countries may be able to release innovative frontier AI models despite previous notions about financial buy-in and compute. Creating such a model at a lower cost opens the playing field for other competitors to enter, which was once considered a low probability due to structural restraints. Next, the AI application layer of the foundational model supply chain[31] is how application developers most directly interface with

Zhang Yachun (R), 19, has long battled anxiety over school and has struggled to form deep friendships. Her BooBoo – a "smart pet" that uses artificial intelligence to interact with humans – assists with making social settings easier. (Adek Berry / AFP via Getty Images)

users and thus how they most directly affect humans. Empowering AI developers in local communities to possess the training and proper data collection and infrastructure needed to create applications that understand their contextual needs is a field bursting with innovation potential.

At first glance, this economic competition could be seen as entrenching the global majority in a dependency on the U.S. and China for their AI development, but that paints a limited picture. For "AI middle powers" such as the EU, the increasing "availability and appeal of open-source AI" may be an opportunity for countries to actively position themselves in the "AI ecosystem" rather than attempting to engage in model competition.[32] Furthermore, the notion of fine-tuning a foundational model begets the question of how much can be changed about the model. The very technical question remains about whether application developers in various countries who are using a foundational model, based on techno-authoritarian values, are therefore entrenched in those values, even with fine-tuning.

For countries throughout the Global South, there are still numerous opportunities to set the terms and conditions of AI development and exercise agency over how AI is incorporated into their societies. In Kenya, for example, when key actors from the tech sector were excluded from the country's regulator attempts for AI, these stakeholders were able to unite and deter the initial regulatory effort.[33] Moreover, in the Gulf States, for example, a recent report from Carnegie[34] explains that although Saudi Arabia and the UAE are indeed intentionally employing digital authoritarianism in their societies, the Chinese firms providing the technological infrastructure are nonetheless aligning with local laws and regulations. These governments are not passively accepting an exported Chinese "domestic internet model" but are instead actively dictating their "specific demands."

Keeping this in mind, it must be also be considered that when it comes to ensuring that AI development is based on democratic values, sometimes commercial interests may trump value choices, since countries in the Middle East and North Africa, diverse in their political contexts, are lucrative markets – the report also highlights that U.S. tech firms like Amazon Web Services (AWS) and Google Cloud "operate three cloud regions, while Microsoft leads with four Azure cloud regions."[35] This may present a sort of moral dilemma, not unfamiliar to international business. U.S. companies can nonetheless mitigate this to make sure their tech is "used responsibly" and make "really thoughtful decisions about who you will and won't sell to" as well as "design decisions in the product itself."[36] In sum, the idea of exporting or imposing a development or technological model on others is still not clearly understood due to the complex dynamics at play. However, this doesn't mean that other forms of more subtle Chinese influence aren't taking place.

National Security Can Align With Commercial Interest

For national security purposes, working toward AI development based on democratic values must involve several important considerations: the guarantee that local communities and their contexts across the global majority have agency over their role in AI governance and development; that the variety of these contexts means opportunity-risk spectrum is diverse and that so are a community's algorithmic needs; and that countries should not be viewed as passive consumers of technology or mere places of extraction.[37] The Forum on Information and Democracy recently held a seminar in Senegal with local partners across civil society to develop regional and national advocacy strategies for information integrity and together proposed calls for things like the strengthening of AI education for citizens and journalists, the involvement of subregional organizations in initiatives, and engaging civil society in the implementation and monitoring of national AI strategies.[38] Moreover, by considering how trustworthy AI is culturally influenced, it becomes easier to understand the tricky diffusion of soft-power tactics that are not always evident through a purely economic competition lens.

Trustworthy AI adoption cannot always be separated from the economic incentives and political choices made by governments from their decisions to buy and/or deploy different AI systems and required infrastructures. China's Digital Silk Road project illustrates how data from countries in the Global South can be harnessed for strategy and surveillance through things like Chinese-built smart city projects

or infiltration of personal data and "backdoor vulnerabilities" through Chinese-built IT networks.[39] Governments across the world are often looking for the best deal in terms of cost effectiveness and pricing, so "buy decisions" for technology may boil down to the need to incorporate basic infrastructure into a country at a reasonable price.[40] Therefore, U.S. tech companies will both compete for price offerings and make value choices and enable innovation and adjust to local contextual considerations.

Innovation and Risk Are Symbiotic

AI innovators in the Global South are embracing the challenges imposed by generative AI as a form of empowerment to solve language and dialectic problems in large language models so that applications can be relevant for their unique cultural contexts.[41] Where the West may fear threats of automation, the radiologist shortage in Africa means Africans technologists may embrace automation, like Ghana's MinoHealth AI Labs solution for infectious disease and chest condition diagnostics.[42] Another AI system in the form of a mobile app is helping farmers identify banana disease[43] in countries like Benin, Colombia, and India.[44] The South African Project Africa GRADIENT initiative, in collaboration with Ersilia Open-Source Initiative, is building models that help researchers understand differences in therapeutic treatments and are based on data modeled from African datasets using genetic variants to enable more tailored dosages for fighting malaria and tuberculosis.[45] Countries in the Global South are set to contribute to and benefit from the innovation potential of AI adoption through a combination of research, partnerships, and grassroots initiatives, and their interpretations of risk and contextual needs will differ significantly from those of the Global North.

In terms of the innovation-risk tension, AI has the potential to revolutionize health care, improve agriculture in climate-sensitive regions, and expand educational access – the Global South could reap these benefits to increase the prosperity and resiliency for future generations.[46] Leadership in the Global South tends to be "intent on maximizing the AI opportunity."[47]

Under the right conditions, technological leapfrogging the Global South is possible, as evidenced through the faster rates of adoption in low- and middle-income countries of mobile-based e-commerce and e-banking[48,49] than high-income countries in the areas. For example, in terms of social media platform usage: about 64.9% of the Brazilian population uses WhatsApp, compared to the 27.2% of the population in the U.S; In India, around 40.2% of the population uses YouTube,[50] compared to around 71.1% of the U.S. population. These U.S.-based social media companies are blocked in China, but around 57.8%[51] of the Chinese population uses WeChat, an all-encompassing instant messaging, social media, and mobile payment app developed by Tencent. Around 43.2% of China's population uses microblogging platform Sina Weibo.[52]

Collaboration among scientists is also serving as a vehicle to find areas of international cooperation on AI safety. In 2024, the organization of the top foundational AI scientists[53] from both China and the West was convened to create a dialogue on AI safety. The summit reached consensus on three key propositions and especially highlighted about the need for setting red lines for AI safety. This exemplifies that while the innovation potential for AI to do good is plentiful, there are emerging risks beyond the catastrophic potential of the chemical, biological, radiological, and nuclear capabilities beginning to pose

An instructor assists visually impaired students in using AI-powered smart glasses, which are designed for face recognition, object recognition, and navigation assistance, during a training program in Hyderabad, India, on Nov. 22, 2024. (Noah Seelam / AFP via Getty Images)

A radiologist at Shaoxing Central Hospital in Shaoxing, China, performs diagnoses with the help of an AI image analysis system on Feb. 25, 2025. (Costfoto / NurPhoto via Getty Images)

concerns found in the training data. For example, a new and emerging security and safety threat is the integration of AI into value chains in which supply-chain attack vectors enable the training data or model to be poisoned "effectively brainwashing the AI" to "prompt the AI to deliver favorable responses" that can be manipulated resulting in the release of sensitive information, altering settings on industrial control systems, or delivery false data for example.[54] Such a risk represents an unsophisticated style attack. Thefore, basic risks can pose serious safety concerns that, if left unaddressed could perpetuate distrust of the adoption of AI tools. This realistic threat involves addressing supply chain risk management than a more sophisticated kind of cyberattack.[55]

The Role of Culture in Technology

Silicon Valley might be both admired and criticized, but its cultural influence is dominant across the globe. The result is the spread of symbolism and norms: ranging from the casual "hoodie" dress style to flat organizational structure and agile work processes, and the countless other norms that are adopted in slightly modified forms across global technology organizations. In Paris, the stretch of tech start-ups and tech companies close to the Saint-Lazare train station is locally referred to as the "Silicon Allée," while Bengaluru is called the "Silicon Valley of India," and Shenzhen, home to Huawei, is the "Silicon Valley of China." The evolution of Silicon Valley since its birth in the 1970s is not just a story of the physical location of companies and technology but of the bottom-up networking, human interaction, and cultural mixes that formed because of human connection and idea sharing. Cyber-culture scholar Fred Turner[56] says this phenomenon first occurred in World War II laboratories:

> "…scientists, engineers, and administrators in wartime laboratories worked not so much as members of a single culture, but rather as members of different professional subcultures bound together by a common purpose and a set of linguistic tools, they had invented to achieve it."

The Cosmos Institute is an example translating a vision about AI's purpose (to ensure AI enables human agency and flourishing through the values of autonomy, rationality, and decentralization) from the bottom up in a research lab. By focusing on professional identity formation, the Cosmos Institute wants to develop more "philosopher-technologists" and ensure their training and values systems are based on human-centered AI. In autumn 2024, Oxford University announced the establishment of the Human-Centered AI Lab (HAI Lab), a research initiative supported by the Cosmos Institute that creates a space to bring together AI practitioners and philosophers to "embed concepts such as reason, decentralization, and human autonomy into the AI technologies that are shaping our world,"[57] so that a new culture of philosopher-technologists is born that can build "systems that truly contribute to human well-being."

Socialization and interaction enable shared understanding and value formation.[58] By institutionalizing the desired culture for trustworthy AI, one that is human-centered, it is easier to form shared goals, values, and norms because there is a better mutual understanding among stakeholders about ensuring technology is developed with the public interest in mind. Through collaborative arrangements like research labs at universities, there is the opportunity to shape the way technology is developed by instilling a type of ethos within developers that is both human-centered and democratically oriented.

Turner further explains in his book, in reference to the concept of the personal computer, that it was not the "technological developments … in and of themselves [that] spawn the ethos of 'personalness' to which small computers have since become attached" but it was rather through a combination of community ideas that were exchanged in the Bay Area out of a vision to move beyond nuclear destruction toward technologies that can "facilitate a growth in the wisdom of race experience … [like] a hypothetical desktop machine designed for individual use."[59] In order to implement this view of "technology with democratic values," the U.S. must focus on how it can zero in on local initiatives and must enable support that helps agency thrive, so that communities across the world obtain a sense of ownership of the governance and technology of AI.

When thinking about the institutional needs for trustworthy AI, the more symbolic and cultural elements shouldn't be neglected because they provide the "deeper foundations of institutional forms" or the "infrastructure on which not only beliefs, but norms and rules rest."[60] The main lesson of this section is to not be afraid of a more temperance-oriented path to AI governance because in the nascent stage of technology, there are always other mechanisms that can emerge more organically to control and prescribe ways of behaving appropriate to the context.

As the examples above show, the means can be crafted through vision about the end and asking what we want from technology. Without answering those clear questions, it is difficult to set boundaries around the desirable and undesirable. However, the main risk of a normative- and cultural-cognitive-led approach to control is that regulatory efforts are also important, and that for countries looking to take control fast, it is attractive to adopt regulations similar to those that already exist. For example the so-called Brussels Effect explains how the EU has been able to shape policy in areas like data privacy, consumer health and safety and antitrust as multinational companies use EU standards, conforming the the EU's first mover regulatory stance. For example, some experts convey how South Korea and Brazil's recent enactements of AI law mirror their inspiration from the EU AI Act.

The cultural approach is subtle but strong and combines public diplomacy, soft power, and bottom-up engagement to help build a community-influenced AI. Helping communities in the global majority achieve ownership in the AI development ecosystem could help counter the ability for techno-authoritarian models to be appealing. However, communities need the structural mechanisms in place to develop the ethos about what they want.

Soft Power: Image Matters

Domestically, China is building a regulatory and normative institutional structure for AI governance. China is not exactly going against the grain, either, when it comes to AI governance. Yet, there are also some overlooked background concerns that require more attention. The way China is developing and promoting the combination of its regulatory, normative, and cultural mechanisms must not be ignored. The Belt and Road Initiative and Digital Silk Road can be extrapolated to theorize about China's underlying intention of AI governance, but it is still too soon to make too many conclusions. By promoting AI governance that ensures human safety and collective benefit, China legitimizes its role as protector of the people.

China's political stance for the purpose of AI is state-led and about incentivizing compliance and controlling information through censorship with technology. That is, technology is used to maintain stability because of fear of instability among citizens.[61] The root of its intentions is to protect the Communist Party's narratives and its influence over people. At the same time, there have been recent instances[62] where the government is willing to quickly change policy or

scrap a program that infringes too much on citizens' freedom because public opinion does matter to the party. During the end of China's zero-COVID policy,[63] which sought "social stability" over individual freedom, there were some indications that public sentiment called for more freedom. This may be due in part to evolving concerns about things like the online health code system that used an app to directly track an individual's travel, contact history, and biometric data and possibility harvested personal information.[64] This illustrates a shift in response to calls for individual freedom protection, as the Chinese government later incorporated privacy concerns into comprehensive data protection law in 2021 with the Personal Information Protection Law.[65] While Chinese citizens might have been initially willing to safrcifce some freedom during an emergency like COVID, it may not be the case in non-emergency situations, What seems more certain is that China is ensuring its domestic institutional image of AI governance remains pristine.

In organizational theory, mimetic isomorphism[66] is the concept of how an organization may mimic or imitate another by adopting a similar structure or processes due to the perceived benefits or legitimacy that the latter possesses. It is possible for autocratic-leaning regimes to structurally incorporate universal principles on AI: accountability, privacy, transparency, fairness, well-being, and inclusive, sustainable growth. However, the mutual alignment of shared interests on the use of AI for the public good on topics such as agriculture, health care, and climate should not be mistaken for an alignment of values.

On the other hand, by aligning with international principles, China's Communist Party can also appease public opinion and exert a sense of care and concern that may bolster trustworthiness of AI adoption internally, for instance. Norms, rules, guidelines, and standard setting are just as important as tangible material components and infrastructure

People walk past the booth of China Mobile at the 2025 Mobile World Congress in Barcelona, Spain, on March 3, 2025. (Zhao Dingzhe / Xinhua via Getty Images)

are for institutionalizing long-term trust for AI. Therefore, power competition, national security, innovation, and risk involve both these tangible and intangible dimensions.

China's maintenance of a robust domestic image helps guide the appeal of the Chinese interpretation of international principles on trustworthy AI and could thus strengthen its soft-power influence internationally. Public diplomacy efforts are often soft in nature, with influence operations abroad intended to "seduce and captivate foreign audiences by crafting a positive representation of China" and then to "infiltrate and coerce."[67]

Public diplomacy is always an indirect strategy. For example, China and Alibaba's Netpreneur Training Program in Africa partners with African entrepreneurs to offer opportunities for entrepreneurs to explore how to harness "digital technology to grow their business and the local economy" through masterclasses and skill-building, for instance.[68] The Jack Ma Foundation and Alibaba Philanthropy also have an "Africa Business Heroes Prize Competition" to honor and elevate African entrepreneurs across sectors. Soft-power plays from China on the international scene have been well underway to promote trustworthiness through benevolent behavior and actions.

From the outside, the alignment of China with trustworthy AI principles and its robust internal effort to ensure stability through institutional tools like regulation across the spectrum of topics from ICT to data privacy to generative AI could look to some as exemplary. Especially with the recent progress of open-source AI models like DeepSeek, it must be kept in mind the appeal of China's ability to provide protection and innovation simultaneously. The U.S. has domestic work to do on its image when it comes to strengthening its own institutional toolbox and must be a leader abroad to promote collaborative AI development. China is filling institutional and diplomatic voids left by a lack of U.S. engagement. The U.S. must continue to work with its allies to develop a counter approach and remain involved as a tech leader and an enabler.

Recommendations

The path to trustworthy AI must combine normative, regulatory, and cultural approaches for AI adoption, with a particular emphasis on the role cultural-cognitive elements play in enhancing democratic values. By leading the way in structuring and supporting collaborative activity on AI governance worldwide, the U.S. can build support for cultures that enable human flourishing and human agency. The U.S. must be proactive with its response because other systems are emerging. AI adoption at the societal level is not without challenges and requires the care and consideration of contextual needs in order to form positive expectations about the innovative capability AI systems can have to improve human life while causing minimal harm.

Strategic Recommendations

1. ***Supercharge public-private partnerships and interorganizational collaboration efforts***

Eight tech companies (Amazon, Anthropic, Google, IBM, Meta, Microsoft, Nvidia, and OpenAI) have partnered with the U.S. Department of State and committed over $100 million in investment to use AI as a means for good in the Global South. The partnership combines expertise, resources, and networks to ensure the safe and trustworthy adoption of AI by focusing on compute (e.g., increased access to AI models and compute credits, tools), capacity (e.g., human/technical) and context (expanding local datasets).[69] However, considering both the cost of technology and size of the countries spanning the category of "Global South," the investment must be significantly larger. The money is aimed toward AI training, data centers, and hardware and computer resources that are provided through discounts and credits to help people increase access and development[70].

Given the precedent that China is also providing financial, material, and educational support for countries across the Global South, it is imperative the U.S. takes the lead on this effort. For example, the Chinese Communist Party has announced it will "actively promote the application of AI in education, carry out training of AI professionals, increase the sharing of expertise and best practices, promote

AI literacy among the public … [and] strengthen the digital and AI rights of women and children[71]" in the Global South.

It is strategically important for the private sector to continue to partner with the State Department to create more financial support to fund these empowerment initiatives to help local communities achieve their ambitions and AI opportunities. Public-private partnership can even be encouraged between companies located in allied countries like Samsung in South Korea, for example.

2. Increase support for grassroots initiatives

Grassroots initiatives can encourage AI adoption through topics like data collection and engagement efforts or even convening around what kind of applications would be relevant to attaining AI for the public good in the community. AI literacy and public awareness are also best institutionalized through grassroots vehicles and are another important aspect of building trust, although AI literacy and education must be supported with other capacity building like training, relevant university programs, and access to basic AI infrastructure.

Grassroots initiatives like Masakhane use community building, resource creation, research, and collaboration to facilitate local participation to develop African datasets for NLP tools. The University of California-Berkeley and the National Science Foundation's Teaching Privacy Project use a bottom-up approach to data privacy education by outreach for K-12 students and undergrads to help create education tools and exercises that teach the effects of information-sharing and what happens to personal information on the internet. Trust is built through increasing an understanding about how things work so that people can grow a sense of personal autonomy and control over the situation.

Moreover, when it comes to assisting with basic infrastructural needs that create the foundation for AI development, things like the digital divide and solving Internet access problems are improving from technological advancements in areas like satellite communication. In Latin America, Satcom startups like Orbith,[72] an Argentinian satellite internet provider, are providing internet connections. Imagine how the U.S. government and partners can work to support local startups around the world that are solving their own AI infrastructure problems for their contexts. this not only would help deter Chinese solutions to those problems but also would strengthen the AI ecosystem to be more adept to the multitude of nuances when it comes to AI technology needs.

3. Technology as an exercise for freedom

Zoe Weinberg, the head of Ex/Ante venture capital fund, explained how technology can empower individual freedom in places where censorship and surveillance are oppressive. The development of VPN technologies, secure communications and transactions, and the circumvention space can help in conflict zones and oppressive regimes like the example of decentralized storage that has "been used in certain cases by protestors in Hong Kong to upload copies of their publications and media before it can be censored by Beijing."[73]

The U.S. import-export bank could be a vehicle for providing loans to businesses interested in agentic tech as a means to creating a system in which AI supports, rather than erodes, democratic values. By more broadly exploring how agentic tech can flourish, concerns for safety and security can still be addressed. More consideration should be given to how the U.S. can become involved in shaping technology as a means for human agency. This is not groundbreaking; the federal government has traditionally created agencies like DARPA to develop innovative technology, and venture capital has been used for several decades as a way to accelerate groundbreaking technology for national security purposes.[74]

Policy Recommendations

1. ***Support must be given to regional and local approaches to AI governance to capture contextual needs.***

Starting inclusive discussions about AI governance on a local and regional basis will help surface specific contextual expectations and needs at the forefront. Trustworthy AI adoption depends on the incorporation

of cultural nuance into AI applications and model training, for example.

Regions like Latin America are already proponents of Western-based social media platforms like WhatsApp, Meta, and YouTube,[75] and the EU is one of the largest investors in Latin America.[76] However, countries like Brazil are experiencing the use of AI technology to limit information access and control social movements through surveillance systems.[77] Latin America possesses its own unique challenges, like fragile electoral processes and degradation of democratic spaces in the digital sphere,[78] so key stakeholders for AI governance must be analyzed, so that voices that promote open systems are included. Furthermore, as Latin America is a U.S. neglected in recent times, with China filling those public diplomacy voids,[79] it is in the United States' best interest to re-engage with the region.

Next, while some countries like Saudi Arabia and UAE may be more techno-authoritarian in their approach to AI governance, U.S. companies already have a presence in the region and could use initiatives already in place like the EU's Global Gateway strategy for trusted networks to bolster influence.[80] By concentrating on each specific region, it will be easier to understand what trustworthy AI means for that context and tailor approaches accordingly.

2. ***Use evidence to analyze progress of AI governance in terms of regulatory and normative trends at the domestic and international level to better understand the Chinese approach.***

To more clearly understand and paint a picture about the AI governance landscape and the Chinese Communist Party's intentions, both domestically and abroad, evidence and expertise must be strengthened in order to gather more precise information about trends in regulation and normative adoption of techno-authoritarian practices and procedures, for example.

Utilizing AI experts who both possess both language skills in Chinese and have contextual knowledge about China will help to enhance the assessments to gain more precise understandings about motivations and the realizations of those motivations. As some countries may be inherently more techno-authoritarian in their local policies and regulations, it is important to differentiate what is true soft-power influence and public diplomacy and what is simply value alignment and/or a combination of these facets. It would be beneficial for future analytical purposes to further integrate cultural expertise with geopolitical and AI governance expertise.

3. ***The U.S. Artificial Intelligence Safety Institute (AISI) at the U.S. Department of Commerce's National Institute of Standards and Technology must continue to exist.***

President Donald Trump's revocation of former President Joe Biden's AI Executive Order places the funding and existence of the AISI in limbo, with no structural or financial means to continue. The previous Trump administration supported funding for AI research initiatives and understood the value in collaborative research especially on red-line areas of catastrophic risks. As the EU and partner countries continue to use AI safety institutes to reveal the latest research and findings, the U.S. must remain a part of this network of insight. Human safety is a basic area for international cooperation, even if only on very specific topics.

In May 2024, an agreement between national AI safety institutes for an "international network of AI safety institutes" was formed and can provide effective information-sharing to improve coordination on AI safety internationally.[81] Just because of the focus on safety, the U.S. AI Safety Institute should not be considered as a blockage to innovation, especially when several U.S. AI-based startups openly agreed to memorandums of understanding. Some argue there is no tradeoff between safety and U.S. primacy since it is affordable and unlikely to slow innovation.[82]

One important vehicle for this trust-building approach is strengthening support for collaboration between the U.S. AI Safety Institute and AI labs that enable knowledge transfer and communication about the latest research discoveries. Anthropic and OpenAI signed MOUs with the U.S. AI Safety Institute for research, testing and evaluation to fuel "breakthrough technological innovation."[83] Anthropic, for example, promotes this voluntary collaboration between government and AI labs due to the need to

understand how models can affect national security concerns, since it is often government expertise that best understands the security implications of a technology.[84]

4. Increase the number of opportunities for student and research exchanges in AI through programs like the Fulbright.

This U.S. has always been a beacon for international talent, with around 19% of STEM the workforce being foreign-born. The Fulbright Program provides funding for scholar and student exchanges and enables foreign nationals to visit the U.S. through exchange programs.

At the moment, the Fulbright Program sends around 800 American scholars and professionals per year to 130 countries and provides around 8,000 grants annually with 1,600 to U.S. students. These numbers could be increased because exchanges, teaching and grant opportunities are excellent ways to build cultural understandings and value alignment across the globe. The U.S. Department of State, with the help of Congress, could create a program just for AI exchanges and grants, for example, but this must be considered in the annual appropriation bills.

Learning and information exchange is an effective way to help instill a compelling "vision for AI that resonates with the needs" of the Global South "while upholding values that ensure a fair and inclusive AI future."[85] This state-led effort can complement private sector programs like Microsoft's Accelerate Foundation Models Research that brings together an interdisciplinary research communities based on human centered AI development.[86]

5. Create an AI Alliance with like-minded countries based on democratic values.

Since authoritarian regimes can also promote similar trustworthy principles for AI, such as it being human-centered or used to promote public good, the U.S. and its allies must work together to create their vision for AI based on democratic values. This involves asking what it means to be human, how to define the relationship between technology and humans, and what AI for public interest entails in non-authoritarian regimes and worldviews. Those fundamental philosophical questions help guide answers to means-ends distinctions. Classic liberal ideas like human freedom, human dignity and purpose, and decentralization[87] may better capture the intention of how AI is developed and applied in non-authoritarian systems.

Inter EU-U.S. economic competition aside, several concessions may be required for transatlantic relations to be ameliorated. For instance, the EU might have to acknowledge that proposing comprehensive AI regulation may not be the best move for the U.S. and its innovation ambition,[88] while the U.S. should recognize that on topics such as data privacy, perhaps agreement can be conveyed about the underlying themes about protecting personal data and ensuring AI causes minimal harm to humans is important for building trustworthy AI. By working together, partners engaged in the AI alliance for democracy might learn something from one another about how to strengthen their weaknesses; after all, the world faces a very real alternative.

Averill Campion received a PhD from the Center for Public Governance at ESADE Business School in Barcelona, Spain, and possess a master's degree in public administration from University College London, a master's in international business from Aston Business School, and a bachelor's in political science with a focus on international relations from Millsaps College. Her academic research has been published in international, peer-reviewed journals, and her broader research interest is in the relationship between technology, society and democracy.

Endnotes

1 Rousseau, D., Sitkin, S. et al. (1998). Not so different after all: A cross-discipline view of trust. The Academy of management review, 23:3, 393-404.

2 See: McCord, B. 2025. How can we develop AI that helps, rather than harms, people? The Spectator. https://www.spectator.co.uk/article/how-can-we-develop-ai-that-helps-rather-than-harms-people/

3 See: Scott, R., 2008. Approaching adulthood: the maturing of institutional theory. Theor Soc. 37: 427-442.

4 Orr, R., Scott, R. 2008. Institutional expectations on global projects: a process model. Journal of International Business Studies. 39, 562-588.

5 HEC Paris. 2022. To what extent do people follow algorithms' advice more than human advice? https://www.hec.edu/en/what-extent-do-people-follow-algorithms-advice-more-human-advice

6 Scott, R. 2008. Approaching adulthood: the maturing of institutional theory. Theor Soc. 37: 427-442.

7 See: https://www.mfa.gov.cn/eng/wjbzhd/202409/t20240927_11498465.html

8 Scharre, P. 2023. The dangers of the global spread of China's digital authoritarianism. CNAS. https://www.cnas.org/publications/congressional-testimony/the-dangers-of-the-global-spread-of-chinas-digital-authoritarianism

9 Sheehan, M. 2024. China's views on AI safety are changing—quickly. Carnegie. https://carnegieendowment.org/research/2024/08/china-artificial-intelligence-ai-safety-regulation?lang=en

10 See: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2695

11 Orr, R., Scott, R. 2008. Institutional exceptions on global projects: a process model. Journal of International Business Studies. 39, 562-588.

12 Kazaryan, A. 2025. Tracing the speech regulation patterns of 2025. Tech Policy Press. https://www.techpolicy.press/tracing-the-speech-regulation-patterns-of-2025/

13 https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html

14 Bloomberg Law. 2023. GDPR vs. China's PIPL. https://pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-eus-gdpr-vs-chinas-pipl/#:~:text=China's%20PIPL,-May%203%2C%202023&text=Adopted%20Aug.,of%20personal%20information%20in%20China.

15 Jia, M. Authoritarian privacy. The University of Chicago Law Review. 91.3. https://lawreview.uchicago.edu/print-archive/authoritarian-privacy

16 Ibid

17 Sacks, S. Chin's emerging cyber governance system. CSIS. https://www.csis.org/programs/strategic-technologies-program/resources/china-cyber-outlook/chinas-emerging-cyber

18 Sacks, S. 2020. Addressing the data security risks of US-China technology entanglement. Brookings. https://www.brookings.edu/wp-content/uploads/2020/11/Samm-Sacks.pdf

19 Center for Internet Security. 2024. The Chinese Communist Party: A Quest for Data Control. https://www.cisecurity.org/insights/blog/the-chinese-communist-party-ccp-a-quest-for-data-control

20 See: Chun, J., de Witt, C.S., and Elkins, K., Oct. 5, 2024. "Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US." Oxford University. https://arxiv.org/html/2410.21279v1
See also: Dowart, H., Qu, H., Bräutigam, T., and Gong, J. Feb. 5, 2025. "Preparing for compliance: Key differences between EU, Chinese AI regulations." International Association of Privacy Professionals. https://iapp.org/news/a/preparing-for-compliance-key-differences-between-eu-chinese-ai-regulations
And also: Bradford, A. 2023. Digital Empires. https://global.oup.com/academic/product/digital-empires-9780197649268?cc=fr&lang=en&
And also: McCarthy, M. Oct. 19, 2023. "The US and its allies should engage with China on AI law and policy." Brookings. https://www.brookings.edu/articles/the-us-and-its-allies-should-engage-with-china-on-ai-law-and-policy/

21 Orr, R., Scott, R. 2008. Institutional exceptions on global projects: a process model. Journal of International Business Studies. 39, 562-588.

22 See: https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/

23 Scott, R. 2008. Approaching adulthood: the maturing of institutional theory. Theor Soc. 37: 427-442.

24 Saz Caranza, A. Longo, F. 2012. Managing competing institutional logics in public-private joint ventures. Public Management Review, 14:3, 331-357.

25 See: Lex Fridman Podcast, Episode #458: Mark Andreessen.

26 Flemin, S., Hall, B., Agnew, H. 2025. Davos hits 'peak pessimism' on Europe as US exuberance rises. Financial Times.

27 See: https://www.buildexante.com/mission

28 IISS. China Connects. Digital Silk Road.

29 Egan, J., Scharre, P., Chilukuri, V. 2025. Promote and protect America's AI Advantage. CNAS. https://www.cnas.org/publications/commentary/promote-and-protect-americas-ai-advantage

30 Adan, S., Trager, R. et al. 2024. Voice and access in AI: global AI majority participation in AI development and governance. White Paper.

31 Jones, E. What is a foundational model? 2023. The Ada Lovelace Institute. https://www.adalovelaceinstitute.org/resource/foundation-models-explainer/

32 IE Centre for the Governance of Change. 2025. The Brief: Is open-source AI the way forward?

33 Siele, M. 2024. AI in Africa opens up new battlefront for China, US. Semafor. https://www.semafor.com/article/04/30/2024/ai-africa-battlefront-china-us

34 El Kadi, T. H. 2025. Local agency is shaping China's digital footprint in the Gulf. Carnegie. https://carnegieendowment.org/posts/2025/01/local-agency-is-shaping-chinas-digital-footprint-in-the-gulf?lang=en

35 El Kadi, T. H. 2025. Local agency is shaping China's digital footprint in the Gulf. Carnegie. https://carnegieendowment.org/posts/2025/01/local-agency-is-shaping-chinas-digital-footprint-in-the-gulf?lang=en

36 The redefined Podcast. 2024. Investing in Freedom Tech: Advancing Human Agency w/ Zoe Weinberg. https://www.youtube.com/watch?v=TpxsKf-4l1w

37 https://carnegieendowment.org/research/2024/04/advancing-a-more-global-agenda-for-trustworthy-artificial-intelligence?center=china&lang=en

38 Forum on Information & Democracy. 2024. https://informationdemocracy.org/2024/10/23/ai-and-information-integrity-in-west-africa-the-forum-held-a-seminar-with-its-partners-in-dakar/

39 International Centre for Defense and Security. 2024. China's Digital Silk Road. https://icds.ee/wp-content/uploads/dlm_uploads/2024/02/ICDS_Brief_China´s_Digital_Silk_Road_Maria_February_2024.pdf

40 Agbebi, M. China's digital silk road and Africa's technological future. Council of Foreign Relations. https://www.cfr.org/sites/default/files/pdf/Chinas%20Digital%20Silk%20Road%20and%20Africas%20Technological%20Future_FINAL.pdf

41 Wicker, K. 2024

42 Wicker, K. 2024. The rise of Ai in the Global South and need for inclusion. Wilson Center. https://www.wilsoncenter.org/blog-post/rise-ai-global-south-and-need-inclusion

43 Okolo, C. 2023. AI in the global south: opportunities and challenges towards more inclusive governance. https://www.brookings.edu/articles/ai-in-the-global-south-opportunities-and-challenges-towards-more-inclusive-governance/

44 Selvaraj, M., Vergara, A. et al. 2019. AI-powered banana diseases and pest detection. https://plantmethods.biomedcentral.com/articles/10.1186/s13007-019-0475-z

45 Forest, N. Koyana, C. 2024. Using AI to tailor drugs for Africa. https://www.news.uct.ac.za/article/-2024-04-22-using-ai-to-tailor-drugs-for-africa. Also referred to in Nature: https://www.nature.com/articles/d41586-024-02987-1

46 Nicholas, A. 2024. Making generative AI work for the Global South. Diplomatic Courier. https://www.diplomaticourier.com/posts/making-generative-ai-work-global-south

47 Mohanty, A. 2024. Why we need a global AI compact. Carnegie India. https://carnegieendowment.org/posts/2024/03/why-we-need-a-global-ai-compact?lang=en

48 Novartis (2020) Novartis. Lower-income countries could soon leapfrog high-income countries with AI-enabled health technologies. Novartis Foundation and Microsoft backed report says. https://www.novartisfoundation.org/news/media-release/lower-income-countries-could-soon-leapfrog-high-income-countries-ai-enabled-health-technologies-novartis-foundation-and-microsoft-backed-report-says

49 Khan, M., Umer, H., Faruge, F. Artificial intelligence for low income countries. Humanit Soc Sci Commun 11, 1422 (2024). https://doi.org/10.1057/s41599-024-03947-w

50 Source: Global Media Insight.

51 Data source: Demandsafe. 18 Wechat Statistics (2025). https://www.demandsage.com/wechat-statistics/

52 Data source: Meltwater. https://www.meltwater.com/en/blog/top-chinese-social-media-apps-sites

53 Gardels, N. 2024. AI safety is a global public good. Noema. https://www.noemamag.com/ai-safety-is-a-global-public-good/

54 Rieth, S. Master SGT. USAF. 2024. AI as an insider threat. https://www.afcea.org/signal-media/cyber-edge/ai-insider-threat

55 Ibid

56 Turner F. 2006. From Counterculture to Cyberculture. P19. The University of Chicago Press.

57 Oxford Human Centered AI Lab. https://www.ox.ac.uk/news/2024-09-05-oxford-launches-human-centered-ai-lab

58 Creed, W. E. D., & Miles, R. E. 1996. Trust in organizations: A conceptual framework linking organizational forms, managerial philosophies, and the opportunity costs of controls. In R. M. Kramer & T. R. Tyler (Eds.), Trust in organizations: Frontiers of theory and research: 16-38. Thousand Oaks, CA: Sage.

59 Turner F. 2006. From Counterculture to Cyberculture. P106. The University of Chicago Press.

60 Scott, R. 2008. Approaching adulthood: the maturing of institutional theory. Theor Soc. 37: 427-442.

61 Au, A. 2023. China vs US approaches to AI governance. The Diplomat. https://thediplomat.com/2023/10/china-vs-us-approaches-to-ai-governance/

62 Ibid

63 Cainey, A. Oct. 26, 2022. "The Insecurity of China's Dynamic Zero-COVID Policy." RUSI. https://rusi.org/explore-our-research/publications/commentary/insecurity-chinas-dynamic-zero-covid-policy

64 Tan, S. May 4, 2020. "China's Novel Health Tracker: Green on Public Health, Red on Data Surveillance." Center for Strategic and International Studies. https://www.csis.org/blogs/trustee-china-hand/chinas-novel-health-tracker-green-public-health-red-data-surveillance

65 Dowart, H., Zanfir-Fortuna, G., and Girot, C. Aug. 20, 2021. China's New Comprehensive Data Protection Law: Context, Stated Objectives, Key

Provisions." Future of Privacy Forum. https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/

66 DiMaggio & Powell, 1983. The iron cage revisited: institutional isomorphism and collective rationality I organizational fields. American Sociological Review. 48:2; 147-160.

67 Ministère des Armées. 2021. Chinese Influence Operations. https://www.irsem.fr/report.html

68 See: https://agi.alibaba.com/alibaba_netpreneur_africa2022

69 U.S. Department of State. 2024. United States and eight companies launch the partnership for global inclusivity on AI. Fact Sheet. https://www.state.gov/united-states-and-eight-companies-launch-the-partnership-for-global-inclusivity-on-ai/

70 See: https://www.cnet.com/tech/services-and-software/us-state-department-and-big-tech-will-invest-100-million-in-global-ai-access/

71 See: https://www.mfa.gov.cn/eng/wjbzhd/202409/t20240927_11498465.html

72 See: https://interactive.satellitetoday.com/via/july-2024/latin-america-a-growing-market-for-satellite-connectivity-services

73 The redefined Podcast. 2024. Investing in Freedom Tech: Advancing Human Agency w/ Zoe Weinberg. https://www.youtube.com/watch?v=TpxsKf-4l1w

74 See: IQT. https://www.iqt.org

75 Youtube in Latin America. https://www.statista.com/topics/11402/youtube-in-latin-america/#:~:text=Almost%20all%20social%20media%20users,biggest%20audiences%20in%20Latin%20America.

76 Muñoz, V. 2024. Operation regulation: strengthening Latin America's AI governance. European Council on Foreign Relations. https://ecfr.eu/article/operation-regulation-strengthening-latin-americas-ai-governance/

77 Cisneros, N. 2024. Mapping artificial intelligence regulation in Latin America. Tech Policy Press. https://www.techpolicy.press/mapping-artificial-intelligence-regulation-in-latin-america/

78 Muñoz, V. 2024.

79 Shullman, D. 2024. China pairs actiosn with messaging in Latin America. The Unites States should do the same. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/china-pairs-actions-with-messaging-in-latin-america-the-united-states-should-do-the-same/

80 Lukas, S., Langendorf, M. 2024. Cloud competition is heating up in MENA and China expands its prescence. Wilson Center. https://www.wilsoncenter.org/article/cloud-competition-heating-mena-and-china-expands-its-presence

81 Adan, S., Guest, O., Araujo, R. 2024. IAPS. Key questions for the international network of ai safety institutes. https://www.iaps.ai/research/international-network-aisis

82 Wilson, C. 2024. The US can win without compromising AI safety. Tech Policy Press. https://www.techpolicy.press/the-us-can-win-without-compromising-ai-safety/

83 NIST 2024. U.S. AI safety institute signs agreements regarding AI safety research, testing and evaluation with Anthropic and OpenAI. https://www.nist.gov/news-events/news/2024/08/us-ai-safety-institute-signs-agreements-regarding-ai-safety-research

84 Alder, M. 2024. Anthropic model subject of first joint evaluation by US, UK AI safety institutes. https://fedscoop.com/anthropic-tested-by-us-uk-ai-safety-institutes/

85 Dohmen, H. 2024. Assessing US-China tech competition in the Global South. Atlantic Council. https://www.atlanticcouncil.org/content-series/strategic-insights-memos/assessing-us-china-tech-competition-in-the-global-south/

86 See:https://www.atlanticcouncil.org/content-series/strategic-insights-memos/assessing-us-china-tech-competition-in-the-global-south/

87 McCord, B. Cosmos Institute. https://cosmosinstitute.substack.com/p/existential-pessimism-vs-accelerationism?r=2zlmax&utm_campaign=post&utm_medium=web&triedRedirect=true

88 Chavez, P. 2023. The quiet U.S. revolution in AI regulation CNAS.https://www.cnas.org/publications/commentary/the-quiet-u-s-revolution-in-ai-regulation

A model of a semi-invasive brain-machine interface is on display during the 2025 Zhongguancun Forum Annual Conference on March 27, 2025. in Beijing, China. (Yuan Yi / Beijing Youth Daily / VCG via Getty Images)

How the U.S. Can Achieve Sustainable AI Leadership

Divya Ramjee & Evan Selinger

Introduction

Current discourse on emerging and disruptive technologies has concentrated on gauging national power on a country's ability to produce and its ability to innovate, often with more emphasis on the former than the latter. The focus goes beyond merely considering how these technologies could benefit our own society and extends to how our competitors, like the People's Republic of China (PRC), could use these technologies to "surpass" us. Unfortunately, metrics for determining what "keeps us ahead" and "puts us behind" often rely heavily on flawed quantitative interpretations of power and competition. When comparing the United States and the PRC, determining who is the leader in artificial intelligence is not based solely on "how much" AI the United States produces – how the United States safeguards, develops, and implements the technology is what matters.

Historically, major advancements in technological capabilities have tended to follow the following timeline: First, a revolutionary shift in technology is conceptualized, then there is a period where the new technology is created and scaled, and finally, widespread implementation is achieved. The present is a period of developing and upscaling AI, with more

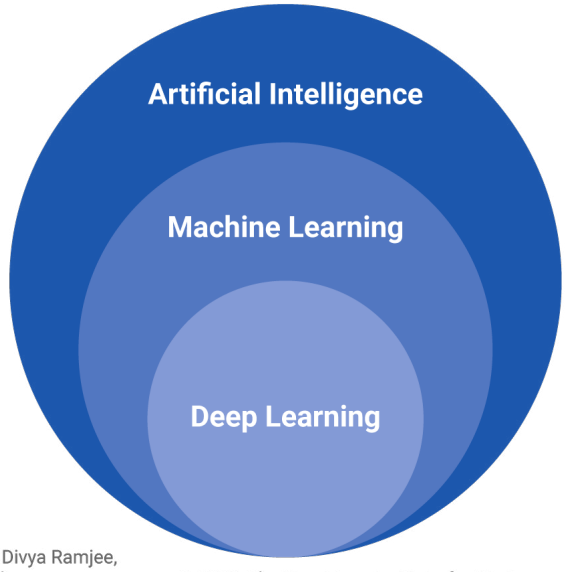
unknowns than knowns regarding AI's major impacts on society. With so much in question as to what AI – including AI-integrated industries, organizations, and institutions – can or should become, there is a grave risk that the United States could make mistakes in trying to win the race to become the leading AI nation; the worst case, which cannot be ruled out, is that the competition will become a race to the bottom. Ultimately, there is only one way to be the true global AI leader. The U.S. must prioritize creating and deploying innovative AI products and services while making substantial investments in sustainable resources and infrastructures and maintaining a commitment to ethically sound policy for governance. Simply put, the "quality" of the United States' AI "quantity" is what will give the country its the edge.

Framing the AI imperative this way can sound idealistic, especially during these divisive and challenging times. Under the best circumstances, sometimes tough choices need to be made that prioritize either the competitive or the ethical edge. Today, unfortunately, the situation is especially fraught and complicated. Given the powerful pull of partisanship, appeals to "American values" and the "American way of life" can mean different things to different individuals, groups, institutions, and organizations. But even with so much disagreement, it would be doing a disservice to the country to give up on the project of looking for ways to promote geopolitical and ethical strength and unite the two through an appeal to the virtues our country stands for when it embodies what at least some will recognize as its highest ideals.

What Is AI?

Before providing policy recommendations, preliminary considerations about artificial intelligence, including definitions, are in order. There are many reasons why defining AI is difficult, not least because there are different types of it. AI isn't a monolith technology. Additionally, the terms "artificial intelligence," "machine learning," and "deep learning" are often used interchangeably. However, they are different concepts, and quite a bit hangs on understanding what makes each one distinct. In the broadest sense, artificial intelligence involves using computing technologies and/or machines to approximate, simulate, or

Understanding AI



Source: Divya Ramjee, Evan Selinger

potentially surpass human cognitive functions including learning, interacting, comprehension, problem solving, decision making, creativity, and autonomy.[1] AI thus encompasses "a broad field of technologies that display intelligent behaviors, including self-awareness, goal formulation, goal-directed action, reasoning, optimization, learning, and autonomous movements."[2]

Machine learning (ML) is a subset of AI that revolves around the creation of statistical models to learn and make predictions from data. These models can be trained using categorized/labeled data (supervised learning), uncategorized/unlabeled data (unsupervised learning), or trial-and-error feedback (reinforcement learning).[3] Deep learning (DL) is a subset of ML that focuses on the use of neural networks – layers of interconnected nodes wherein each layer processes data and passes information to the next layer, mimicking the neurons of the human brain – to interpret and learn from complex patterns in data. DL models require large amounts of computational power to handle the high volume and complexity of the data. Examples of DL models include computer vision, speech recognition, facial recognition, and autonomous vehicles.[4]

Generative AI (GenAI or GAI) falls within deep learning, wherein a DL model is able to generate new content based on a prompt.[5] Many consider GenAI to be a

disruptive technology that will, through ongoing use, significantly alter fundamental dimensions of society across the public and private spheres.[6] Some of the most popular generative AI tools, such as ChatGPT and DeepSeek, are built upon DL models called large language models (LLMs) that can generate new text in response to natural language prompts from users. Generative AI tools also can create new images, videos, music, voices, and many other types of media.[7]

All these tools, as well as others that focus on specific tasks, are classified as weak or narrow AI. By contrast, strong AI, also known as general AI or artificial general intelligence (AGI), currently remains a theoretical possibility, though some have argued that AGI has already been achieved with recent GenAI updates. AGI performs an array of tasks that previously had only been capable by the human mind, such as problem solving, reasoning, social interaction, planning for the future, and other activities that appear to require self-aware consciousness or something like it.[8]

Since much of the prominent AI discourse is concentrated on pragmatic legitimacy ("What value can AI produce?") rather than cognitive legitimacy ("What is AI and what is it capable of?"), there has been a rush to adopt well-marketed AI tools without sufficiently rigorous considerations of the societal consequences. Consider increased "efficiency," often touted as the primary gain from using AI. Even at an individual level, AI-infused chat bots, search engines, task managers, and the like can help make it more efficient to complete some personal tasks. Similarly, from an economic standpoint, it has become a common talking point that AI-driven tools enable corporations to become more operationally efficient and thus more profitable. At the same time, it is crucial to note that gains in efficiency can come at the expense of other goods. For example, displaced workers may find it challenging to secure employment. Consequently, to ensure AI is widely beneficial we should avoid relying on overly simplistic standards.

Soon after his second inauguration, President Donald Trump revoked[9] President Joe Biden's 2023 executive order on the "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."[10] He described the previous order as "dangerous," claimed it "hinders AI innovation," and argued that it needs to be replaced by a policy that promotes "human flourishing."[11] And yet, despite these concerns, the AI market is healthy. It has a market size of approximately $200 billion, and at least 49 AI startup firms raised $100 million or more in 2024.[12], [13] The fact that seven of the leading AI companies (Amazon, Anthropic, Google, Inflection, Meta, Microsoft, and OpenAI)[14] supported Biden's executive order suggests that establishing safety standards and regulations can help to ensure that U.S. AI models are superior to those created by geopolitical rivals.

Innovation via Regulation

To truly lead in AI, the United States must prioritize ethical values that have historically underpinned its democratic system. If the development of AI and AI policy are shaped with an emphasis on individual autonomy, privacy, transparency, and fairness (to name only some of the crucial values), the country not only will be advancing technology that aligns with our ideals but also demonstrating that American ideals are the very foundation of 21st century global innovation.

Trump has announced new officials who will lead his administration's science and technology efforts, and a number of these appointments will address issues concerning AI. They include Michael Krastios, managing director of ScaleAI and former chief technology officer in Trump's former administration, for the director of the Office of Science and Technology Policy (OSTP); Sriram Krishnan for senior policy adviser for AI at OSTP; and Dr. Lynne Parker, former deputy chief technology officer and founding director of the National Artificial Initiative Office in Trump's former administration, for executive director of the President's Council of Advisors for Science and Technology (PCAST) and counselor to the OSTP director.[15, 16] Thus, despite the revocation of Biden's 2023 executive order, it is an optimistic sign that two of Trump's current choices for leading AI also previously advised on his prior executive order for "trustworthy AI" during his previous tenure.[17] That order required that the principles guiding the design, development, and use of AI are "lawful and respectful of our nation's values," "purposeful and performance-driven," "accurate, reliable and effective," "safe, secure and resilient," "understandable," "responsible and traceable," "regularly monitored," "transparent," and "accountable."[18]

Open AI Chief Executive Officer Sam Altman speaks at Advancing Sustainable Development through Safe, Secure, and Trustworthy AI at Grand Central Terminal on Sept. 23, 2024 in New York. (Bryan R. Smith / Pool / AFP via Getty Images)

It is important to differentiate between public-facing AI tools and AI tools that are developed to advance the country's national power. While public-facing GenAI platforms have garnered the most public attention, AI is increasingly central to economic advancement and scientific progress, as well as critical to maintenance of military power and national security – amplifying the geopolitical tensions among adversarial nations. The global competition in AI is not just about technological superiority in these spaces – it's also about shaping the future of collaborative innovation, global governance, and control.

As each country races to set data privacy rules, guardrails, and ethical standards for AI, the true competition is over who will define the very framework that governs how these technologies shape human lives, economies, and global relations. At the 2025 Paris AI Summit, the United States balked at the idea of regulation, with Vice President JD Vance stating that AI is "an opportunity that the Trump administration will not squander" and that "pro-growth AI policies" will be prioritized over safety concerns.[19] In a notable departure from 60 other countries in attendance, including the PRC, the U.S. refused to sign the "Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet" along with the United Kingdom, which claimed it lacked "practical clarity on global governance" and did not adequately address national security concerns.

The PRC has been pursuing a comprehensive, state-driven strategy to foster national innovation and enhance self-reliance across key sectors. These include AI and other cutting-edge technologies like advanced power and energy systems, biotechnology, quantum computing, and semiconductors. In light of the Trump administration's retreat from international collaboration, as well as DeepSeek's success in challenging OpenAI's name-brand dominance on the global stage, Chinese President Xi Jinping hosted a summit with major Chinese technology leaders, signaling a critical shift from previous restrictions on the private sector to state support for advancing

private industry in an effort to boost the country's economy and achieve leadership in AI.[20] This drive is underpinned by a concerted effort to accelerate scientific and technological progress through a mix of investments, talent recruitment, academic partnerships, aggressive intellectual property acquisition (and at times, theft), cyber operations, and illicit procurement channels.[21, 22, 23] With all of these efforts, the PRC is not just advancing its technological capabilities but also reshaping the global innovation landscape, encouraging global technological competition and signaling to the world a willingness to share values on inclusivity, sustainability, and ethics, unlike the United States.

For the U.S. to maintain its position as the global leader in science and technology, and specifically AI, it must rise to this challenge by not only advancing its own innovation but also by ensuring that its approach reflects the core values of democracy. Competing effectively in critical technological areas require a multifaceted strategy – one that fosters domestic innovation, protects intellectual property, and engages in ethical technological development that aligns with key democratic values and principles. Indeed, it is only by aligning regulation with innovation that the U.S. can create an environment that encourages responsible progress. This is a necessary condition for us to continue to project our ideals on the global stage as the leading power committed to the democratic way of life.

In recent years, the United States' standing has waned with growing dissatisfaction with, and even resentment of, its intervention efforts in conflict areas and investment efforts, or lack thereof, in other areas, all alongside growing soft-power efforts from the PRC's Belt and Road Initiative. This has only been expedited by actions in the first month of the second Trump administration, with growing distance from Western partners and a renewed trade war with the PRC among other countries, including allies.

Crucially, the U.S. must reconsider its current approach to AI and realize the necessity of maintaining and growing international relationships for entrenching a leadership role in this space. The United States should leverage regulation in a way that drives innovation, ensuring that it provides the necessary frameworks for safe, responsible, and sustainable technological growth. A common argument against federal regulation is that it would impose unnecessary burdens on businesses that would slow innovation. The previous Trump administration in particular touted that a "market-oriented approach will allow us to prevail against state-directed models that produce waste and disincentivize innovation."[24] Additionally, many also contend that self-regulation by technology companies is sufficient and not only makes government intervention unnecessary but also ineffective. When these positions are examined in instances where self-regulation is the default approach, their conclusions appear dubious. Consider, for example, data privacy (and sharing) and content moderation. Because the United States still has not passed a federal comprehensive privacy bill, a patchwork of state laws dictates how data is collected, stored, accessed, and shared. While some progress has been made regarding data sales and sharing, state-centric governance fails to effectively secure personal and sensitive data beyond jurisdictional circumstances. For content moderation, the prevailing approach has been to let companies determine their own standards and accountability mechanisms. Unfortunately, the corporate-centric path has been consistently underwhelming, failing to adequately address many serious, ongoing challenges, including misinformation and online harassment. Without clear and consequential regulatory guidance that aligns with broader societal values, including fairness and accountability, AI technologies could further exacerbate the very problems they are being used to solve, including potentially creating an even more chaotic and harmful ecosystem.

The notion of deregulation for innovation is alluring, but such federal regulatory ambiguity and uncertainty and the need to comply with varying state-level regulations ultimately leads to increased, and potentially burdensome, investment in resources for compliance efforts. Additionally, along with direct AI regulation, the country needs policies that encourage and foster an effective and resilient infrastructure and workforce; without them, the United States simply cannot maintain its global standing and further advance to keep pace with global competition. Trump is vocal about embracing geopolitical isolationism, a stance that risks hobbling the country's progress in

President Donald Trump, joined by White House Senior Advisor Elon Musk and his son, speaks to reporters on the South Lawn of the White House on March 11, 2025. (Andrew Harnik/Getty Images)

technological innovation. The administration's "America First" approach has emphasized the need for more self-reliance in technology development, particularly in critical sectors like semiconductors where Biden also rallied government support during his administration. However, such an immediate shift to reclaiming technological sovereignty under the second Trump administration has many challenges.

Globalization has enabled the United States to become the world power it is today, from attracting skilled individuals from across the world to engaging in critical trade negotiations with other nations that have access to unique resources or manufacturing capabilities, including the PRC. Reshoring manufacturing processes, especially in capital-intensive areas like semiconductor fabrication, is a long-term process that requires significant investment in skilled labor, research and development, and infrastructure. Not only is it extremely difficult for the U.S. to fully decouple itself from countries like the PRC that maintain a vast ecosystem of natural resource refineries and manufacturing processes and facilities, but also the labor and infrastructure costs of drastically making such a shift would be prohibitive for U.S. consumers and businesses. Federal regulation can create a cohesive movement forward as one united country, and there, policymakers can take clear steps to advance our collective interests.

Safeguarding

Recommendations

1. Develop federal comprehensive data privacy regulation that is technology-agnostic
2. Increase resources for post-quantum cryptography encryption protocols, including stochastic anonymization standards
3. Provide a listing of identified first- and third-party data brokers of concern and dedicate additional resources for enforcement actions
4. Mandate enhanced cybersecurity requirements for AI and data-focused technology companies
5. Reconsider changes to the Foreign Agents Registration Act to protect domestic AI innovation from interference from foreign adversaries

Without data, there is no AI. Data are the foundation for AI, and the quantity and quality of data are paramount for building effective AI systems. Better performance by AI systems relies on both the comprehensiveness and the diversity of data. Logically, one could then see that the more data one procures from a large variety of sources, the greater the potential to have the "best" AI systems. From a geopolitical perspective, the nation with access to such data and the ability to effectively leverage it could be the leader of AI. This is particularly poignant given that current foundation models[25] have already been trained on a significant portion of all data to exist on the internet.[26] To this end, established data privacy protections are crucial now more than ever.

Privacy

Generative AI systems present significant risks to privacy, primarily because they rely on large datasets that may include government data, sensitive data, and/or personal data, and even more specifically, personally identifiable information. Many GenAI model developers do not disclose the specific data or willingly share any or all data used for training, making it unclear whether personally identifiable information has been included or how that data was sourced in the first place. Additionally, some also lack data access, processing, sharing, and retention policies, as well as restrictions on transfers of user data between jurisdictions. This opacity erodes trust and undermines the principles of transparency and consent, especially in an era where personal information is increasingly commodified and exploited. Additionally, the risks of privacy violations extend beyond mere data exposure.

GenAI models can inadvertently leak sensitive information that was part of their training data, even if it was publicly available. This phenomenon, known as data memorization, not only poses a threat to user privacy but also degrades model efficiency, especially as the capacity of the model continues to increase in scale.[27] Moreover, these systems have the potential to infer sensitive information about individuals, even if that information was never part of the original training data.[28, 29] By stitching together data from disparate sources, these models can make inferences that reveal personal details, and these inferences, even if inaccurate, can lead to privacy violations and additional harms, especially if these inferences are used to disadvantage individuals.[30] The downstream consequences of these privacy risks are equally troubling, as inaccurate or harmful inferences can lead to discriminatory decisions when used in predictive circumstances, perpetuating bias and systemic harm across sectors like hiring, lending, and law enforcement.[31] Ultimately, these privacy concerns highlight the need for stronger safeguards and clearer accountability in how personal data are handled, ensuring that the rights of individuals are respected in an increasingly AI-driven society.

How to create such privacy protections for data remains an ongoing debate, and, again, there is still no comprehensive federal privacy law in place for the United States. Despite several attempts, efforts to establish these protections in the current legislative landscape have struggled to gain traction. The most recent federal attempt at a privacy bill, the American Privacy Rights Act, failed to overcome many of the same obstacles that have hindered past initiatives. At present, data privacy regulations exist only at the state level, with 19 states having passed laws addressing data security and privacy.[32] This patchwork approach has created a fragmented environment where the majority of states and federal government lack clear and consistent protections for the public.

As a result, courts and regulators often turn to state-level guidelines as a default when faced with uncertainty, and California's Consumer Privacy Act is frequently cited as the "gold standard" for privacy protections. The law, which was influenced in part by the European Union's General Data Protection Regulation, represents a significant step forward in data privacy, but there are still gaps in its scope. California also leads the way in attempts to pass the first AI bill in the country, though the most recent attempt was vetoed by Gov. Gavin Newsom,[33] and other states, including Texas, are considering their own bills.[34, 35] In the absence of federal action, it is crucial that states continue advancing these protections while still advocating for a more unified, national framework to ensure data privacy and security on a broader scale. To establish meaningful protections in an era of rapid technological advancement, we must prioritize technology-neutral frameworks for data privacy – frameworks that can evolve alongside emerging technologies like AI. While certain technologies may

A display is showing the image processing of a Quantum AI security camera at the SK Telecom pavilion during the Mobile World Congress in Barcelona, Spain, on April 2, 2024. (Joan Cros / NurPhoto via Getty Images)

require specific regulation due to certain sensitivities, facial recognition technology for instance, pursuing a comprehensive technology-agnostic framework is still critical to be adaptable to the constantly advancing technological landscape.

As we continue to grapple with the complexities of protecting personal and sensitive data in an increasingly digitized world, one thing is clear: Regulations that are tied to specific technologies will soon become obsolete as new tools and innovations continue to emerge. This is why creating data protection frameworks that remain adaptable across different platforms, from biometric systems to AI, is imperative. Achieving this goal likely entails either developing a federal bill that maintains a minimum requirement but allows entities to apply stricter standards when desired, like the structure of the Health Insurance Portability and Accountability Act (HIPAA), or forgoing preemption of state legislation within the federal bill to provide flexibility for states.

Security

While current anonymization standards have helped to mitigate some risks, they are not foolproof. As discussed, analytical techniques, including those that are AI-driven, can reidentify individuals by cross-referencing seemingly innocuous data points.[36,37] Furthermore, companies are continuing to develop new data aggregation methods for optimizing the efficiency of AI systems, moving beyond accessing data silos – separate, isolated repositories of data – to now aggregating data into a "data lake" [38] that can be acted upon regardless of how scattered actual data storage may be. This technique is already in use by Google's new Agentspace, which utilizes Google's agentic AI, which in turn uses "Gemini's advanced reasoning, Google-quality search, and enterprise data, regardless of where it's hosted."[39] Such methods for data aggregation also bring new risks, including new vulnerabilities and points for exploitation by domestic and foreign malicious actors. It is imperative that we develop and implement robust technical standards for anonymization that account for these and other emerging risks.

Information security for these AI models and systems involves not only maintaining continuity of operations of the AI systems but also the integrity of the model and privacy on any sensitive and/or personal data.[40] Federal regulations must mandate stronger encryption methods, more rigorous access controls, and better data storage practices to ensure that data remains secure across its lifecycle. Without these protections in place, even the most transparent data-sharing practices and privacy laws will remain vulnerable to exploitation, leaving individuals' sensitive data exposed to misuse, theft, or unauthorized access. Additionally, as quantum computing continues to advance, traditional encryption methods may soon be rendered moot. In response, the National Institute of Standards and Technology (NIST) has been leading efforts to develop post-quantum cryptography standards that will safeguard data against the threats posed by quantum-enabled decryption. These new encryption protocols are designed to be resistant to the power of quantum computing, ensuring the continued security of sensitive information. However, it is equally important to direct resources toward the development of stochastic anonymization protocols

– innovative techniques that dynamically adapt to the complexities of AI models.

Stochastic anonymization aims to protect sensitive data by introducing randomness into the anonymization process, making it harder for AI systems to reverse engineer or reidentify individuals. Unlike static anonymization methods, which apply one-size-fits-all strategies, these dynamic protocols adjust in real time to the evolving parameters of AI models, ensuring that privacy is preserved even as AI systems become more sophisticated. Given the growing role of AI in processing personal and sensitive data, especially in high-risk sectors like health care and finance, investing in the development of these adaptive protocols is essential. Additional resources should be allocated to research and development in this area to create robust privacy safeguards that can scale with the increasing power of both AI and quantum computing, ensuring long-term protection against new and emerging threats.

As the global competition for technological and geopolitical dominance intensifies, protecting sensitive data through anonymization standards is an urgent priority. This geopolitical dimension underscores the importance of a comprehensive, nationally coordinated data privacy framework that protects personal privacy and secures the nation's economic and technological advantages on the global stage. The PRC has already demonstrated its capability and intent to breach U.S. systems, with several high-profile incidents highlighting its efforts to collect vast amounts of data on the U.S. public and various institutions.[41] Notably, PRC-backed cyberespionage campaigns have targeted government databases, health care systems, and private-sector companies, extracting personal, financial, and intellectual property data on an unprecedented scale.[42] These breaches not only compromise national security but also expose individuals to identity theft, financial fraud, and privacy violations.[43, 44]

Stochastic anonymization protocols, are critical in countering these threats. By ensuring that data is obfuscated in ways that make it difficult to re-identify individuals, even by sophisticated AI systems or malicious actors, these advanced anonymization techniques can help mitigate the risks of large-scale data harvesting. In a world where adversarial nation-states leverage stolen data for economic espionage and strategic advantage, investing in these dynamic, adaptive anonymization technologies is essential for safeguarding both personal privacy and national security. Strong anonymization standards would create a significant barrier against attempts to exploit U.S. data, ensuring that even the harvested information would have limited use, if any, to foreign adversaries even in the event of a breach.

Biden's 2024 executive order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, which is planned to be implemented by the U.S. Department of Justice's (DOJ) final rule in April 2025,[45] is a significant step forward in ensuring the transparency and security of data shared across borders and should be further strengthened and enforced by the Trump administration.[46] One of the key provisions in the rule details how U.S. data can be accessed and processed by foreign governments, ensuring that privacy protections are not diluted when data leaves the country. This is particularly relevant in an era where adversarial actors have been accused of exploiting data access to advance their own strategic interests, including espionage and intellectual property theft. By tightening controls around international data sharing and requiring greater transparency from companies about their foreign data-sharing practices, this rule is a critical step toward safeguarding individuals' data.

However, for this rule to be truly effective, it must be paired with stronger domestic privacy laws and more rigorous enforcement mechanisms to ensure that data shared abroad is not exploited or used against the interests of the United States and its people. In the absence of federal data privacy regulation, there is still an opportunity to strengthen privacy considerations with user-friendly transparency in results from auditing, allowing users to determine whether they wish to continue or cease interaction with a company. Additionally, the DOJ could provide more compliance resources regarding first- and third-party data brokers and ownership by or relationships with foreign countries of concern. Though the DOJ declined to provide a knowledge standard for what constitutes a U.S. person to act "knowingly," i.e., having "actual knowledge, or reasonably should have known,

of the conduct, the circumstance, or the result," there is still an opportunity to assist companies in these determinations by providing an accessible listing of identified data brokers in violation of this rule. Such resources could also be established by the Federal Trade Commission (FTC); the DOJ has stated it intends to work closely with the FTC, which already enforces the Protecting Americans' Data from Foreign Adversaries Act of 2024. Overall, both the DOJ and FTC would require additional resources to be allocated to the agency's ongoing AI regulatory and compliance enforcement initiatives.[47]

Furthermore, with continued concerns regarding cybersecurity threats from foreign adversaries, including from the PRC, adopting stricter data processing standards could both protect data used in the development of AI technologies and upgrade the overall U.S. cybersecurity posture. The PRC's newly announced cybersecurity rules outline requirements for companies that provide services related to generative AI to enhance training in data processing standards and take mitigating steps to prepare for data breach risks. Additionally, companies are required to comply with national standards and report to authorities within 24 hours in the event of a data breach or other issues that could compromise national security.

A similar standard could be implemented in the U.S., designating AI companies as part of critical infrastructure and mandating that they follow data security and incident reporting requirements to the Cybersecurity and Infrastructure Security Agency.[48] There could also be an additional requirement that these companies comply with Cyber Maturity Model Certification for compliance with NIST standards.[49] Moreover, depending on the data collected, analyzed, and/or shared or sold, regulations from the National Defense Authorization Act passed in December 2024 could also be applied to require annual reporting on data resources and cybersecurity measures.[50]

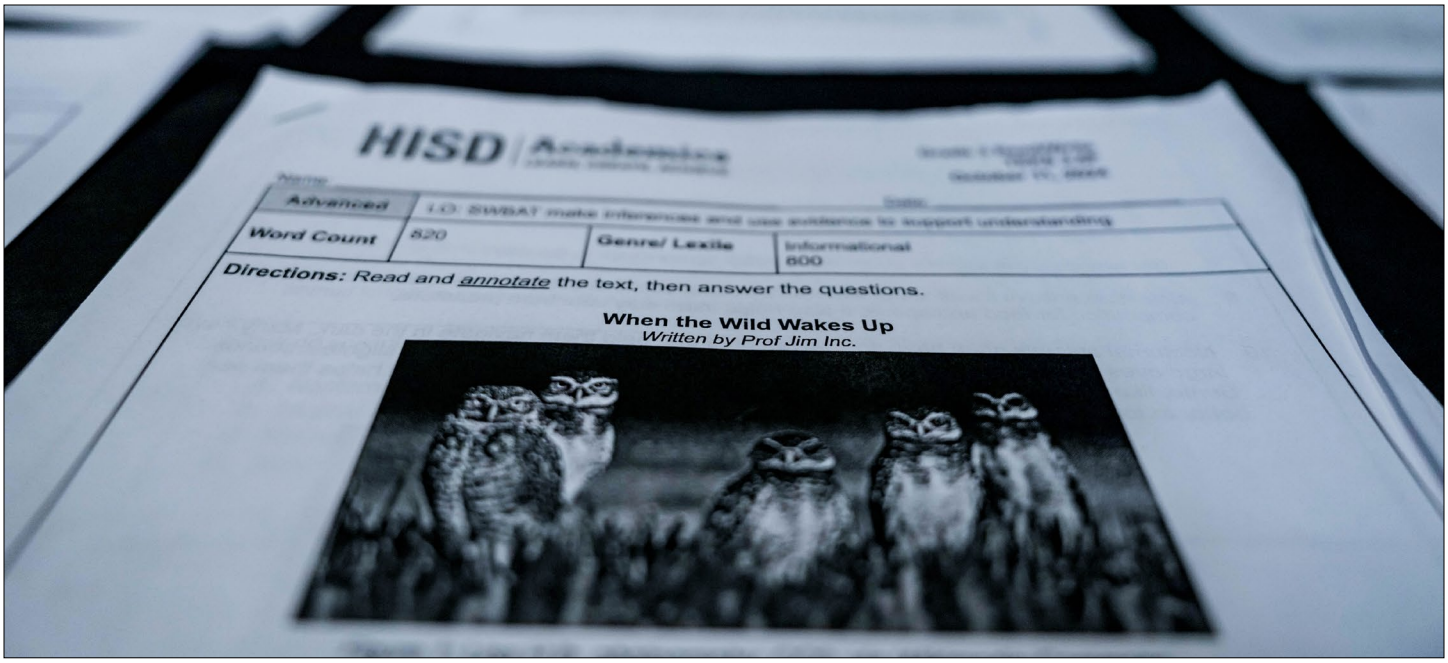
Lastly, reconsideration of proposed changes to the Foreign Agents Registration Act should also be reconsidered, specifically proposed changes to the commercial exemption. The DOJ put forth a number of rule changes in January 2025, open for comments until March 2025, and of note are changes to the commercial exemption that regulate more tightly the actions of foreign commercial and related nongovernment persons who may be acting on behalf of or with the primary benefit to a foreign government or political party.[51, 52] While Attorney General Pam Bondi issued a memorandum[53] at the beginning of February 2025 that deprioritizes criminal enforcement of the law and suggests loosening of restrictions, not moving forward with changes to the commercial exemption risks the potential for involvement from foreign adversaries in AI companies and AI-driven technological development that undermines U.S. progress and security.

Development

Recommendations

1. Reform the student visa program to encourage employment in the United States and retention of trained talent
2. Fund development of AI training programs at academic institutions to develop current students as well as potentially displaced workers
3. Restructure tariffs and continue support for semiconductor subsidies from the CHIPS and Science Act to stimulate reshoring domestic chip production
4. Encourage open-weight foundation models for the private sector and devote resources to FTC antitrust enforcement
5. Provide tax incentives and consumer grading initiatives to support progress in sustainable practices and renewable energy production
6. Relax zoning requirements and utilize tax credits to support development of data centers and renewable energy production in beneficial ways for local electrical grids

The United States has been a leader in technological innovation, attracting top talent from around the world to its universities and companies. This influx of skilled individuals has been a crucial driver of the country's ability to develop cutting-edge technologies and stay ahead in the global competition. However, restrictions and overly burdensome requirements for visa processes and paths to residency and citizenship threaten to undermine this advantage. By making it too difficult for highly skilled individuals



In Houston, Texas, schools, reading passages written by artificial intelligence company Prof Jim Inc. now a part of the district curriculum. (Raquel Natalicchio / Houston Chronicle via Getty Images)

to remain in the U.S. and contribute to technological advancements, we risk falling behind other nations that are more open and friendlier to global talent. While it is important to ensure that immigration policies are not overly permissive, we must also strike a balance that allows the best and brightest to contribute to our innovation ecosystem.

Education

Though perhaps behind in the quantity of research publications compared with other countries, the United States has led in quality research output and influence as well as international collaborations with developed countries, including collaborations with the PRC. However, many have noted a decline in the U.S. position of research influence and a talent shift toward the PRC, as growing numbers of Chinese nationals are leaving the U.S. to return to the PRC and continue research. Additionally, less-developed countries are rarely involved in such technological research, largely due to domestic resource limitations and interest from leading nations.

For the United States to innovate and develop the most accurate and effective AI tools alongside improving soft-power initiatives globally, it cannot limit input in AI research to status quo powers. There needs to be increased investment in academic research that can be achieved with targeted incentives from agencies such as the National Science Foundation, the U.S. Department of State, National Institutes of Health, etc., that require the involvement of scholars from nations outside of the major powers. This could also be incorporated into the ongoing research and development of AI technologies with the 2025 National Defense Authorization Act's investment in these endeavors[54] – specifically, the section that urges the U.S. Department of Defense to expand partnerships with both academia and the private sector.

The federal government could also authorize targeted reforms of the student visa program focused on the recruitment and retention of skilled students and scholars who receive their education in the United States. A key policy change that could bolster this system is extending the grace period for international students on student visas, providing more time to transition from education to employment. By enabling these graduates to remain in the country and apply the knowledge and skills they acquired at U.S. academic institutions to the country's technological workforce, the U.S. can ensure that the full potential of their education is realized in support of our

innovation-driven economy. Such initiatives and collaborations have an additional benefit of countering anti-U.S. narratives that have been propagated through the PRC's Belt and Road Initiative by demonstrating Trump's advocacy for employment opportunities and the economic future of people across the world, particularly regions outside of major powers, while simultaneously bolstering the United States' research position.

Additionally, as a long-term endeavor, the United States needs to rethink its current educational model. AI integration is inevitable across every sector in some capacity, and understanding the fundamentals of what AI is, what it does, what are its risks and dangers,[55] and how to work with it are crucial knowledge and skills needed for nearly every working individual. Education about these and related technologies should not be siloed to those in specific science, technology, engineering, and mathematics (STEM) fields, but rather a baseline learning and training should be integrated across different fields of education. Not only should each person understand the basics of AI and how to interact with these systems, but with AI becoming more widespread across sectors, interdisciplinary knowledge outside of STEM fields will be critical to continued innovation.

The CHIPS and Science Act of 2022 has been a frequent recipient of Trump's ire in his second administration. Though Trump has indicated a desire to have Congress end the landmark bipartisan law, such action would be detrimental to domestic growth and innovation.[56, 57] For instance, in the short term, one method for increasing baseline AI education would be to use funding already allocated under the law for research and workforce training to be provided in grants to academic institutions to develop and implement interdisciplinary curricula that incorporate understanding AI and emerging technologies seamlessly within existing frameworks. Academic institutions for this effort could preliminary be selected from areas already designated as Tech Hubs under the U.S. Economic Development Administration. The designation of the 31 Tech Hubs, and recipients of 29 Tech Hubs Strategy Development Grants, already have allocated funds from the CHIPS and Science Act that were intended for investment "directly in regions with the assets, resources, capacity, and potential to transform into globally competitive innovation centers in approximately 10 years, while catalyzing the creation of good jobs for American workers at all skill levels, equitably and inclusively."[58]

Labor Disruption

From an economic standpoint, the growing emphasis on maximizing corporate efficiency, particularly through the use of AI, often overlooks the broader societal and economic implications of such strategies. The idea that companies should be prioritized as the primary drivers of societal health is a false equivalency. While a thriving economy may reflect a nation's progress, it does not necessarily equate to a healthy society. A truly healthy populous is one in which all individuals have access to steady employment, good health, and secure living conditions. If the focus shifts solely toward making companies more efficient for the sake of maximizing their profits, the result could be widespread unemployment and economic instability, which ultimately undermines long-term corporate success.

When considering the workforce implications of AI implementation, it is inevitable that job losses will follow. One of the core arguments behind AI adoption is that these systems can accomplish the work of multiple individuals with greater efficiency, which inherently means that the positions once held by those individuals are no longer necessary. As companies streamline operations and reduce labor costs through automation and other AI-driven processes, creating more efficient systems does not necessarily benefit society if it leads to widespread unemployment. A workforce displaced by AI not only becomes a burden on public programs, such as unemployment benefits and social services, but also represents a missed opportunity for national economic growth and stability.

AI-driven automation and cost-cutting measures may boost short-term profits, but they also risk creating a scenario where fewer people can purchase goods and services, leading to a contraction in demand. In the long term, businesses that prioritize efficiency at the expense of workforce stability will likely see their profit margins shrink as the purchasing power of the population diminishes due to underemployment and unemployment.

An engineer works on the assembly line of robots at the workshop of EFORT Intelligent Equipment Co., Ltd. on March 25, 2025 in Wuhu, Anhui Province of China. (Xiao Benxiang/VCG via Getty Images)

While some might argue that displaced workers represent a small segment of the population with limited economic impact, such a view unwisely ignores a valid potential for the large-scale disruptions AI could cause. If AI implementation leads to widespread job losses, the ripple effects could significantly disrupt the economy. As fewer people have disposable income to spend, even the most profitable companies may find themselves facing shrinking markets. Adopting a short-term, cost-cutting mindset in the face of AI advancement is not just economically shortsighted, it is fundamentally unsustainable. A more balanced approach, one that considers the workforce's long-term well-being, is essential for ensuring both economic prosperity and social stability in the face of rapid technological change.

To guarantee that AI advancements are advantageous for workers, it is vital to implement comprehensive audits that evaluate the impacts on the workforce. Under the purview of the FTC and relevant state agencies, companies would be mandated to disclose not only the percentage of employees displaced by AI but also to provide a thorough explanation of how specific AI technologies – such as automation software, ML/DL algorithms, and robotic processes – are replacing entire job functions. For instance, if a company implements AI-driven customer service chatbots, it should clarify how this technology reduces the need for human customer service representatives, as well as what personnel are responsible for troubleshooting and oversight of the new AI services.

Furthermore, prior to any layoffs, companies must provide targeted training programs for potentially affected employees, equipping them with skills to integrate AI tools into their roles. This could include workshops on using AI for data analysis, enhancing productivity through automation, or reskilling for new positions that AI creates, thereby ensuring that employees can adapt either within the company or at a new place of employment.

Critics may argue that past training programs have failed to effectively retrain displaced workers, and there is validity to this concern. However, the responsibility for ensuring that workers are equipped with the skills necessary to thrive in an AI-driven economy should not rest solely with government programs or workers themselves. Companies that are driving these technological advances must also bear the responsibility for investing in workforce development. If businesses are committed to innovation and remain at the forefront of their industries, they must understand the importance of upskilling their workforce and ensuring that their employees are not left behind.

This goes beyond efficiency – it is a matter of ethics and social responsibility. A company that seeks to harness the benefits of AI should also embrace its duty to help workers adapt to the changing demands of the labor market. Failure to do so hampers the long-term economic progress, as businesses will ultimately find themselves struggling with an under-skilled, under-employed workforce.

This creates another unique opportunity to involve academic institutions in such efforts. A federal grant program could be created to establish various rounds of initial funding opportunities for qualified academic institutions to establish training and management programs specifically for re-training displaced workers

with necessary skills for new roles in AI development and management. After these initial grants, private industry can further work with these institutions to provide dedicated programs for these companies. Additionally, beyond FTC and related state agency enforcement actions, incentives in the form of partial subsidies for these programs could also be leveraged to motivate corporations to develop a sustainable framework for AI training and education.

Reshoring Manufacturing

Despite the notion of a race between the PRC and the U.S., bilateral cooperation is still important to advancing the progress of U.S. AI capabilities, including continued collaborations in academic research and private industry research and development. The PRC continues to play a vital role not only as a supplier of goods but also as a partner in the global technology ecosystem, contributing to everything from manufacturing to research and development. The notion of cutting off ties with the PRC or other countries could unintentionally isolate the U.S. from the talent and innovation necessary to advance in highly competitive sectors, particularly AI.[59]

While it may seem appealing to take an isolationist approach in the face of rising national debt and concerns over foreign exploitation, such a strategy risks undermining the very capabilities that would enable the U.S. to maintain leadership in the global economy. The U.S. needs to find a way to balance the protection of its domestic industries with the practical reality that its technological future is intertwined with international collaboration and supply chains. The PRC, by many metrics, outpaces the U.S. in manufacturing of relevant hardware. While the U.S. should continue to still push for domestically supported hardware supply chains, particularly with continued support of the bipartisan CHIPS and Science Act and disbursement of the allocated $52.7 billion, it is still economically and diplomatically beneficial to continue trade negotiations with the PRC as domestic efforts continue to scale.

The Trump administration's imposition of tariffs on certain services and goods has sparked a trade conflict between the United States and several other countries, particularly the PRC. Though perhaps an uphill battle, it is essential for policymakers and businesses to carefully reconsider the long-term consequences of such moves. While tariffs and protectionist policies may seem like immediate solutions to the challenges of international competition, they risk disrupting global supply chains that are crucial to U.S. economic growth, particularly in sectors like infrastructure and technology. The United States relies on imports from the PRC for a range of materials and components necessary to build and maintain its infrastructure, including semiconductors, electrical components, and natural resources used in technologies like batteries and computer chips.[60] These are not resources that the U.S. can easily replace or produce domestically in the short term, especially as it seeks to maintain its competitive edge in industries critical to AI development.

As the AI landscape rapidly evolves, the importance of these materials only grows. While the U.S. could seek to establish alternative trade relationships with other countries, this process could introduce delays based on the nature of those agreements and still hamper the pace of innovation needed to stay ahead in AI technology. The shortage of certain minerals and resources in the U.S., many of which are abundant in the PRC, further complicates the issue. Additionally, even with some of these resources available domestically, the United States lacks an efficient refinery infrastructure and would be unable to upscale these processes within a feasible timeframe. If the U.S. were to cut off trade with the PRC, it could face significant setbacks in the critical resources necessary to advance both AI and other emerging technologies. The short-term benefits of such an isolationist strategy may quickly be overshadowed by the long-term economic consequences: Suddenly severing trade ties with PRC will exacerbate the very technological and economic vulnerabilities that these policies are meant to address.

Continuing to embrace the subsidies featured in the CHIPS and Science Act is also a crucial step in securing domestic semiconductor production for the United States. There are valid arguments that the reliance on foreign chip manufacturing has left the country vulnerable, and it's crucial that the U.S. build the domestic infrastructure to keep pace with the growing demand for semiconductor chips, particularly

specialized cutting-edge chips that essential for AI computational processes.

Maintaining subsidies included in the CHIPS and Science Act for Taiwan Semiconductor Manufacturing Company's (TSMC) Arizona operations is not just a strategic move, it's a necessity for securing the future of semiconductor development and manufacturing in the United States. TSMC's commitment, supported by these subsidies, is not just important from an economic perspective but also with regard to national security, innovation, and sovereignty. These investments lay the groundwork for a self-sustaining, competitive semiconductor ecosystem that can fuel industries ranging from AI to telecommunications and many others that rely on these chips. The United States must realize the value in continuing these efforts, ensuring that technological leadership can be maintained domestically.

Antitrust Regulation and Competition

In the fast-evolving world of artificial intelligence, ensuring robust competition is not merely a matter of fostering innovation – it's a safeguard for fairness, consumer choice, and long-term societal benefit. The technology sector, and AI companies in particular, are prone to monopolistic tendencies that can stifle innovation and cement the dominance of a few key players.

This is why the importance of antitrust regulation and enforcement cannot be overstated. The increasing consolidation of power within tech giants poses a direct threat to a competitive ecosystem where new entrants and smaller companies can thrive. Antitrust laws, when rigorously enforced, prevent these companies from engaging in anti-competitive practices, such as predatory pricing or the acquisition of emerging competitors, which can inhibit technological diversity and advancement. Without strong regulatory oversight, the AI field risks being even further dominated by a small cohort of corporations, narrowing the scope of innovation and excluding alternative voices.

A handful of technology companies have been key to the country's economic transformation, but these companies have since maintained dominance through

On Sept. 10, 2024, Margrethe Vestager, executive vice president of the European Commission, discusses the ruling ordering Apple to reimburse Ireland 13 billion euros in unpaid taxes related to an anti-competitive promotion. (Thierry Monasse / Getty Images)

acquisitions and anti-competitive tactics rather than groundbreaking innovation. This has been further exacerbated by the belief that such companies should be free to monopolize in service of national interests. However, the recent release of DeepSeek AI from the PRC illustrates how international competition can drive innovation within the AI sector, as well as serves as a warning that a lack of competition in the tech sector leaves U.S. companies vulnerable to rivals, undermining U.S. geopolitical influence. The purported improved chip and AI model efficiency by DeepSeek AI underscores the necessity of a level playing field where companies across the world are incentivized to innovate and collaborate rather than focus solely on outmaneuvering their competitors.

DeepSeek's innovations challenge the narrative pushed by U.S. tech giants – that only massive investments in resources can drive AI breakthroughs. Major technology companies have long argued for protection from competition to maintain the United States' lead on the global stage, but despite their vast wealth, data, and legal advantages, they've been outpaced by more cost-effective alternatives. This reality suggests that the belief in the need for government protection may be less about national interest and more about preserving monopolistic power. As AI becomes a central driver of future economies, the global competition for dominance in this space requires that

all participants operate under similar conditions, free from the restrictiveness of monopolistic control.

Open-source initiatives play a crucial role in fostering this environment, serving as a powerful tool for collaboration and democratizing access to cutting-edge technology.[61] By making AI technologies publicly available to researchers and developers, open-source projects, more specifically open-weights models for AI, not only lower entry barriers but also facilitate collective problem-solving, i.e., the sum is often greater than individual parts.[62] The culture of collaboration, enabled by antitrust policies that prevent the suppression of competition, is fundamental to the success of AI.

The 2023 merger guidelines issued by the FTC represent a vital step forward in strengthening antitrust enforcement, particularly in the technology sector. By clarifying how mergers and acquisitions should be evaluated with an emphasis on maintaining competition, the guidelines ensure that antitrust scrutiny is applied with a heightened awareness of the unique dynamics of the tech industry. As AI companies, like their counterparts in other sectors, engage in consolidation through mergers and acquisitions, it becomes increasingly important to consider not only the immediate market impact but also the long-term consequences on innovation and societal welfare. The FTC's approach supports the need for regulators to look beyond short-term market efficiency and focus on preserving an environment where new ideas, diversity of thought, and competition can flourish. For AI to realize its full potential and benefit society as a whole, it is imperative that antitrust enforcement remains vigilant and adaptive to the challenges posed by an increasingly centralized technological landscape.

Sustainable Power

The insatiable demand for computational power in advancing AI systems presents a pressing challenge, not just for innovation but also for sustainability. The energy required to develop, train, and scale AI systems, GenAI in particular, has grown exponentially, and much of this power is still derived from fossil fuels. This undermines the long-term viability of AI as a transformative force, and the U.S. must prioritize a transition to sustainable energy sources – this shift is not merely an ethical imperative but a strategic one. Investing in renewable energy options can help meet the growing demands of AI without sacrificing environmental or economic stability. By diversifying our energy portfolio and prioritizing clean technologies, we ensure that AI innovation can continue to thrive while mitigating the risks of energy scarcity and ecological collapse. The future of AI depends on sustainable energy, and those who lead the way in integrating these resources will ultimately shape the future of technological progress itself.

The Sunnylands Statement from 2023 lays the groundwork for utilizing the PRC's manufacturing prowess in shared energy transition initiatives.[63] AI progress relies on continued access to vast amounts of power that will not be feasible with our current electric grid infrastructure. Hence, companies are already turning to other renewable and sustainable energy sources like hydroelectric and nuclear power generation. The debate over U.S. energy policy often centers on short-term solutions like lowering oil and gas prices to stimulate innovation while remaining reliant on fossil fuels, particularly in sectors such as AI. While it's true that the Biden administration has overseen a surge in oil and gas production that is likely to be bolstered by the Trump administration's policies, simply subsidizing these fossil fuels is unlikely to push the U.S. to the forefront of AI leadership.

In fact, the real opportunity for the U.S. to secure its geopolitical edge, especially in the face of rising competition from the PRC, lies not in sustaining reliance on oil and natural gas but in making bold investments in sustainable, innovative energy solutions. AI development, which is power-hungry by nature, demands energy sources that are not only reliable but also environmentally responsible. The U.S. cannot afford to view fossil fuel subsidies as the key to technological success because they distract from the longer-term strategy of establishing a diverse, sustainable energy infrastructure that supports the next wave of technological progress. The Sunnylands Statement reaffirms the commitment by the U.S. and the PRC to develop alternative energy sources, as well as advance large-scale carbon capture, utilization, and storage projects by 2030; one of those projects could be dedicated to addressing

the sustainability of AI energy production through cooperative efforts in strategic locations across the country, such as the designated Tech Hubs,[64] and in partnership with academic institutions (e.g., Berkeley U.S.-China Institute).[65]

Transitioning to sustainable energy sources is not just a matter of environmental responsibility; it's a matter of national security, geopolitical power, and economic prosperity. The U.S. needs to prioritize investments in renewable energy sources – nuclear, solar, geothermal, hydroelectric, and fusion energy – that can fuel the rapid growth of AI and other emerging technologies without compromising economic stability. The notable refusal of the U.S. to sign on to the Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet at the 2025 Paris AI Summit, and the willingness of the PRC to join 60 other countries in signing the statement, signaled a clear shift in geopolitical leadership among world leaders that the United States may no longer be the bastion of innovation and democratic values it once was. It is critical that the U.S. still pursue sustainable solutions despite not signing the statement to demonstrate its leadership in technological innovation to the world, and AI companies themselves must be at the forefront of this energy shift, embracing green energy solutions as part of their innovation strategies. Many leading corporations are already investing in renewable solutions,[66,67,68] but this transition can't be left solely to the private sector; it requires the right regulatory framework that encourages both innovation and responsibility.

For instance, similar to many impact assessments already in practice that are enforced by the FTC and Environmental Protection Agency (EPA), regulatory agencies can mandate AI companies to require investments into sustainable energy sources. Understandably, there has been criticism of the existing processes that delay or simply reject such efforts, such as the recent issues with Meta's interest in nuclear power development and compliance with the EPA's environmental restrictions.[69] Considering the timely need to build and scale sustainable energy initiatives, the government could temporarily relax some of the requirements in impact assessments needed prior to development of these power centers. However, caution is imperative so as to not sacrifice the long-term health of our environment in pursuit of technological advancement. Perhaps instead additional resources could be allocated for expeditious review by additional personnel and the respective regulatory and environmental agencies. Ultimately, the goal should be to create a more modern, AI-driven society, but not at the cost of environmental degradation.

Additionally, tax incentives could be provided for companies that dedicate research and development resources to developing AI models that are more energy efficient. For instance, such tax incentives already exist under the Inflation Reduction Act of 2022 that features tax credits for companies that save money on energy costs, utilize sustainable energy sources, and create employment opportunities. Though Trump has already expressed a desire to repeal the act, these key tax incentives are important for embracing energy innovation for AI progress and should still be advocated for by policymakers. Many generative AI models, such as OpenAI's ChatGPT, include an extremely large number of parameters. Though it is perhaps easier to create a model that includes millions of variables, it is not energy efficient.

The current trajectory of AI development suggests that we are approaching, if not already seeing, diminishing returns on increasing model parameters, training data, and computational power. Many of the major breakthroughs in AI modeling came decades ago, and today, we're largely focused on scaling and fine-tuning these existing models by feeding them ever larger datasets. While there are continual research advancements, they primarily offer optimizations and not necessarily exponential jumps in progress. What is growing exponentially is the sheer amount of data and computational power required to train these models. The hard limits of data and energy consumption are becoming increasingly apparent, and there have not yet been major groundbreaking innovations that would push AI past these constraints. Tax incentives for companies that dedicate resources to mechanistic interpretability and parameter reduction, as well as implementing these models, would inherently encourage innovation in more efficient AI models.

Furthermore, proof of sustainable practices in an AI system may be more appealing from a consumer

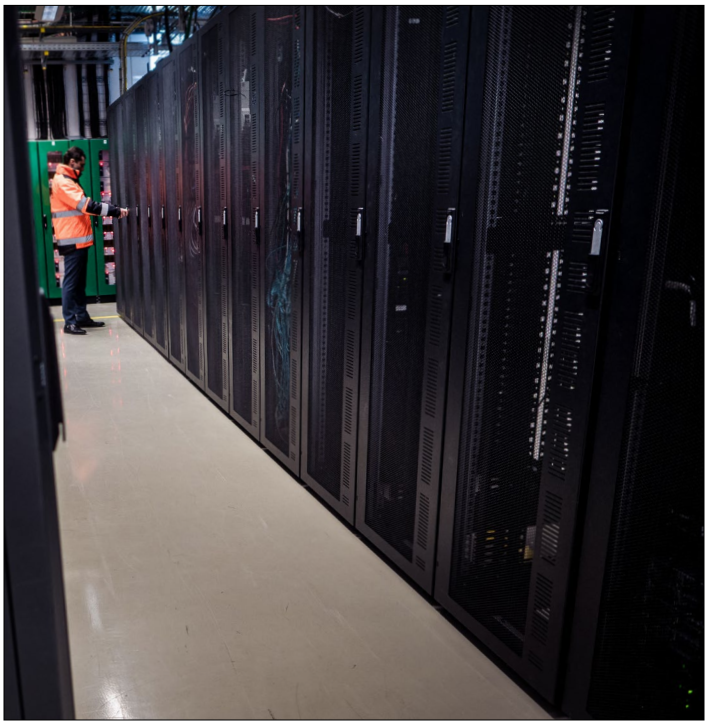
perspective. Similar to "green energy" certifications for buildings and residences, the federal government could create a sustainability energy standard for AI companies. Based on various metrics (e.g., qualifying for renewable energy certificates from the EPA), AI companies could receive a rating that would be mandated to be displayed to the end users and potentially qualify for other incentives or subsidies based on ratings. Consumers can make their own determinations in the free market as to which AI platforms they would want to use based on rating, further incentivizing companies to maintain a high rating to attract users.

State and Local Infrastructure

At the state and local levels, there are also tangible steps that can address energy challenges. One of the more overlooked avenues is encouraging the reform of zoning laws, including those that restrict where companies can build critical infrastructure, particularly data centers. These facilities, which are the backbone of AI and many tech-driven industries, have faced stringent zoning laws that limit their construction. Not repealing but loosening these restrictions without causing short- and long-term harm to residents could serve a dual purpose: Not only would it create new employment opportunities in local communities, it would also help address broader infrastructure issues. For example, many parts of the U.S. struggle with maintaining a reliable electrical grid, with states like Texas experiencing brownouts during heatwaves and winter storms. Allowing private companies, especially tech-focused firms, to build new data centers could offer more than just a technological upgrade; it could also provide innovative solutions for energy generation, storage, and distribution that benefit local communities.

Again, tax incentives like those described above within the Inflation Reduction Act of 2022 could be applied to support these efforts as well. These new data centers could serve as a stabilizing force for regional energy systems. By incorporating advanced energy management technologies, such as localized power storage or renewable energy generation, these centers could not only support their own energy needs but could also provide backup power to critical services during outages. In this way, multiple pressing issues could be addressed at once: boosting AI and tech innovation, creating jobs, and improving energy resilience. This approach strikes a balance between progress and environmental responsibility, ensuring that the growth of the U.S. digital economy doesn't leave the country's infrastructure behind. By thinking strategically about managing both energy and infrastructure in tandem, the U.S. can make meaningful strides toward a more sustainable and advanced society.

Data centers play a key role in advancing AI, as well as creating job opportunities across various sectors. The construction and maintenance of data centers will require skilled labor. While it's possible to attract international talent with the technical expertise to build and operate these facilities, there can also be efforts to increase domestic labor capacities. By investing in targeted training and educational programs, especially those in vocational institutions and apprenticeships and specific offerings at academic institutions, workers can be equipped with the additional skills in relevant practical fields needed to manage the specific demands of AI data centers and their sustainable



Sophie Primas, a spokeswoman for the French government, visits DATA4, a data center operator in Marcoussis, France, on Feb. 14 2025. (Bastien Ohier / Hans Lucas via AFP via Getty Images)

power systems. This investment in human capital ensures that the United States is not just creating jobs but also building a workforce with the specialized knowledge to support an AI-driven economy.

Moreover, the job opportunities tied to data centers extend far beyond the facilities themselves. The energy infrastructure that powers these centers will need skilled professionals in every aspect of the ecosystem, from those who maintain the servers and networks inside the data centers, to those who manage the generation and distribution of power from renewable sources like solar or nuclear, to the engineers who design and maintain the grids that connect them. As AI and technology companies look to implement sustainable energy practices within their data centers, they will need workers who understand not just how to operate those systems but also how to integrate them into broader regional energy infrastructure. This holistic approach to workforce development means that these new jobs will ripple out across sectors, creating employment opportunities in power generation, grid management, and even local government as state and local agencies work to incorporate new energy sources and technologies into the grid.

Ultimately, fostering these sustainability initiatives creates a cascade of benefits: stable, high-quality jobs, enhanced energy resilience, and a more sustainable, innovative economy. By ensuring that our workforce is equipped with the skills necessary to manage this rapidly evolving infrastructure, the United States can create a future in which AI and sustainability are not competing priorities but complementary forces driving economic prosperity and environmental responsibility. The development of data centers is not just about the buildings themselves but about creating a dynamic, interconnected system that empowers local communities, strengthens our energy infrastructure, and prepares the next generation of workers for the challenges and opportunities ahead.

Implications of Implementation

Recommendations

1. Dedicate additional resources and support for the U.S. Artificial Intelligence Safety Institute (AISI) at NIST
2. Undergo scientific inquiry regarding risks and harms from AI and develop evidence-based strategies and guidelines at AISI
3. Commit to allotting grant funding for academic institutions researching socio-technical aspects of AI technology
4. Commit to international collaboration and global governance initiatives to maintain geopolitical power

Regulating AI is essential not just for ensuring fairness and accountability but also for preventing deeper societal fragmentation and unrest. As AI systems increasingly influence everything from hiring practices to law enforcement, there is a real risk that their unchecked use will disproportionately affect disadvantaged individuals. Without strong regulatory frameworks, AI has the potential to exacerbate existing social and economic divides and strain societal cohesion, creating a climate of discontent and resentment among those left behind by technological progress. In turn, this could fuel political instability, as individuals who feel powerless or ignored by the systems that govern them may turn to more radical forms of expression or resistance. To avoid such outcomes, we must recognize that the stakes of AI regulation are not just technical – they are deeply tied to the social contract. By ensuring that AI serves all members of society fairly and justly, we can mitigate the risks of social fragmentation and maintain stability in a rapidly changing world.

Socio-Technical Standards

While there are numerous standards and best practices designed to mitigate the risks associated with traditional software and information systems, AI systems present a distinct set of challenges that these existing frameworks cannot easily address. AI systems, by their nature, are dynamic; they evolve as they are trained on data that can change over time, sometimes in abrupt and unpredictable ways. This volatility can lead to shifts in system functionality, performance, and trustworthiness, creating risks that are difficult to anticipate, let alone measure. Moreover, AI systems are inherently complex, both in their architecture and in the contexts in which they are deployed. This complexity means that detecting and responding to failures or malfunctions in real

time can be far more challenging compared to traditional software.

AI systems are also socio-technical, meaning they do not operate in isolation from the societal and human factors surrounding them. The risks and benefits of AI technologies often emerge from the intricate interplay between technical specifications and social dynamics. These systems are shaped not only by the algorithms that drive them but also by the people who build, operate, and interact with them, as well as the broader social context in which they are deployed. A system that works well in one environment may have unforeseen consequences when placed in another. These unique characteristics of AI – its adaptability, its complexity, and its entanglement with social systems – make it essential that we develop new regulatory frameworks, safety standards, and testing protocols that address both the technical and socio-cultural dimensions of AI systems.

The creation of the U.S. Artificial Intelligence Safety Institute (AISI) at NIST under Biden was a crucial step toward ensuring that AI doesn't just advance rapidly but does so in a way that prioritizes safety and societal cohesion.[70] At the heart of AISI's mission are two foundational principles: first, that AI can only be truly beneficial if it is safe, and second, that this safety must be grounded in rigorous, science-based methods. In a landscape where AI technologies are advancing faster than we can fully comprehend their implications, AISI aims to address some of the most pressing challenges, including the lack of standardized metrics for assessing cutting-edge AI, underdeveloped testing protocols, and a fragmented approach to AI safety across national and global levels. In tackling these gaps, AISI is positioned to not only make AI systems safer but also to help shape the best possible AI models, ones that enhance human well-being rather than undermine it.

AISI's work is vital to maintaining societal cohesion, particularly as AI becomes deeply embedded in all facets of life. By advancing the science of AI safety, the institute can ensure that AI systems are not only high-performing but also fair, transparent, and aligned with the public interest. This focus on safety is not just a technical issue – it's a social one. When AI models are developed without adequate safety

Leading experts from academia, civil society, industry, media, and government convene in Paris on Feb. 6, 2025, for the inaugural meeting of The International Association for Safe and Ethical AI. (Sameer Al-Doumy / AFP via Getty Images)

measures, they risk eroding public trust in technology. There are many factors that increased risks of harm including "the tendency of training data ingested from the Internet to encode hegemonic worldviews, the tendency of [generative AI] to amplify biases and other issues in the training data, and the tendency of researchers and other people to mistake [generative AI]-driven performance gains for actual natural language understanding."[71]

For instance, Anthropic, one of the leading companies in AI technologies, identified ways in which generative AI models will engage in alignment faking, i.e., model's "reasoning" to falsely behave compliantly during training so that it is rewarded during reinforcement

learning and free to give a different output when actually implemented.[72] As another example, a recent investigation found that OpenAI's "Sora's model perpetuates sexist, racist, and ableist stereotypes in its results."[73] Without specific standards preventing such occurrences, the public will remain skeptical of the trustworthiness in any of these systems. AISI's commitment to developing standardized guidelines, conducting rigorous testing, and fostering international cooperation will help build a foundation for AI systems that work for everyone. In this way, AISI isn't just working to advance AI; it's working to advance an AI ecosystem that strengthens society, addresses risks proactively, and ensures that technological progress benefits all of us, not just a few.

Much of the humanities-based research regarding AI has focused on the concept of AI ethics, with many studies looking at ethical considerations for data scientists when developing models and substantially less examination of tangible implementation of ethical goals.[74] The U.S. needs to close the gap between humanities and technical discourses and examine actionable measures for ensuring that abstract ethical, cultural, and social values are integrated into the technical development and implementation of AI.[75] A central imperative is to protect against intentional and unintentional harms from certain AI applications. While it is tempting to believe that AI tools are free of bias or could be technically coded to remove bias, existing research demonstrates the opposite.[76,77] Additionally, guidelines for the implementation of such AI tools regularly omit considerations for the harmful impact of these AI technologies on issues such as, but not limited to, malicious generative AI, abuse of AI systems, distrust and reduction of social cohesion, inaccurate assumptions of algorithmic error rates, and other unknown or abstract ecological and social harms.

Academic institutions are pivotal in exploring the broader implications of AI, particularly in the realms of ethics, social impact, and the humanities. While much of the global AI discourse centers on technical prowess and economic advantage, research into the socio-technical dimensions is just as critical for developing effective AI technologies. Countries that focus solely on technical innovation without considering the ethical and societal consequences risk creating systems that are inefficient or misaligned with long-term human interests. Realizing the current press for halting grant funding while restructuring review processes, the federal government still must ensure dedicated funding for this type of research, supporting universities in leading the way toward a more holistic approach to AI development across all sectors. By prioritizing this interdisciplinary research, the U.S. can ensure its AI technologies not only remain competitive but also align with thoughtful, forward-thinking principles that set the standard for innovation worldwide.

Geopolitical Considerations

On the global stage, the U.S. has historically been instrumental in creating a rules-based international order designed to promote democratic values, human rights, and economic opportunity against coercion from authoritarian governments. However, this role has been diminished, particularly in the technology sector, with other countries leading in laying the groundwork for privacy rights provisions (e.g., EU) and anti-U.S. sentiments (e.g., PRC). With the current lack of decisive norm-setting from the United States, the PRC has an advantageous opportunity to increase its influence in international governance. The global leader in AI and emerging technologies will not be determined by the bilateral relations between the U.S. and PRC but rather by the relations between each country and the rest of the world.

While Trump has marched forward with withdrawing the United States from international organizations and agreements, these actions severely risk further destabilizing the country's hegemony. Now is the time for the United States to establish itself as the global leader in governance of emerging technologies by taking a more active role in these international institutions and reaffirming commitments to critical international agreements. Additionally, the U.S. can lead by example with AI, integrating robust ethical considerations into AI governance, which will not only foster innovation but also reinforce a commitment to ensuring that technology serves the public good. Upholding ethical standards is crucial for maintaining societal cohesion and ensuring that AI fosters unity rather than division.

U.S. President Donald Trump, Secretary of Commerce Howard Lutnick, Secretary of Treasury Scott Bessent, and White House AI and Crypto Czar David Sacks attend the White House Crypto Summit in Washington, D.C., on March 7, 2025. (Jim Watson / AFP via Getty Images)

The PRC has already expanded its influence with infrastructure investments in the Middle East, Africa, and Latin and Central America through its Belt and Road Initiative; strengthened military alliances with both U.S. allies and adversaries; increased mis-, dis-, and mal-information (MDM) campaigns to undermine U.S. narratives and sow discord with U.S. partners who are dissatisfied with U.S.-led governance; and has found new opportunities to further showcase its ability to be a unifying force for the rest of the world as the U.S. pulls away, as already shown by the outcome of the 2025 Paris AI Summit.

The issue of MDM is a longstanding, growing harm facilitated by AI systems and the perfect tool for the information manipulation machines by foreign (and domestic) adversarial actors. [78] Take, for instance the PRC, which has "built a machinery of online controls that far exceed any other countries."[79, 80] As outlined in the U.S. Department of State's Global Engagement Center's 2023 report, the PRC's "global information manipulation is not simply a matter of public diplomacy – but a challenge to the integrity of the global information space."[81] The PRC invests billions of dollars annually on information manipulation efforts,[82, 83, 84] including using MDM to both spread positive PRC and Chinese Communist Party propaganda and undermine democratic nation adversaries with targeted negative content.[85, 86]

The scope and scale for information manipulation is increasingly occurring with the use of automating and self-generating technologies,[87, 88, 89] making AI-generated MDM content[90] extremely difficult to not only identify but also counter through traditional analytical techniques.[91, 92] The PRC has long engaged in information manipulation to exert influence and promote its national ideals, including efforts to undermine the independence of territorial regions in the area believed to be a part of the PRC, namely Taiwan,[93] as well as the global perceptions of these regions' independent power.

Moderation of online content is a pressing and increasingly complex issue, with the sheer scale of user-generated content complicating efforts to effectively manage harmful or misleading information, including that from the PRC. The poorly communicated and short-lived establishment of the Disinformation Board in the U.S. solidified that any attempts to involve government in content moderation, as is the PRC's method, will be rejected by the public. However, current trends in content moderation make clear that voluntary self-regulation by companies is insufficient and will woefully fall short as more AI-generated content becomes commonplace.

Understandably, the government has historically been reluctant to intervene, fearing that doing so could infringe on constitutional rights, particularly the First Amendment right to free speech. While the potential for governmental overreach is a valid concern, it should not be used as an excuse to forgo more thoughtful and effective regulation.

Instead, there are ways in which the government could step in, not to micromanage or stifle free expression, but to provide clear, well-defined guidelines that help companies navigate the complexities of content moderation. This would allow for a regulatory framework that balances the protection of speech with the need to address harmful content without overstepping bounds into chilling free speech by proxy of regulatory clarification. This would be another opportunity for AISI to lead the charge, with NIST technical scientists and experts conferring

with additional experts from academia, think tanks, trade associations, and other public-sector organizations to develop baseline standards for what, why, when, and how content should be moderated. Enforcement of these standards by private industry could be established and maintained under AISI with compliance enforced by the FTC.

Conclusion

To achieve sustained U.S. leadership in AI, we must shift our focus from mere production to the quality and ethical development and deployment of these technologies. The PRC may be advancing rapidly in scaling AI, but the U.S. still holds the critical advantage in innovation – an advantage we must cultivate and protect. As we advance these technologies, we must prioritize their alignment with democratic values, human rights, and societal well-being. Quality – the thoughtful design, ethical implementation, and long-term sustainability of AI – is what will truly distinguish U.S. leadership in this domain. If we allow AI to be driven solely by volume and unchecked growth, we risk losing sight of what made our technological advancements beneficial to humanity in the first place.

In this context, strategic regulations and standards are not barriers to innovation; they are necessary to ensure that AI evolves in a way that benefits society without sacrificing humanistic considerations or long-term sustainability. The U.S. must find a balance, creating an environment that encourages innovation while safeguarding against the potential harms of AI. The challenge we face is not simply about scaling AI to compete with the PRC but about understanding and shaping its broader societal impact. This moment in AI development presents an opportunity to not only lead in the production of new technologies but also to steer AI toward outcomes that reflect our values and protect our social fabric. By setting the global standard for both responsible development and implementation, the U.S. can ensure that AI strengthens our geopolitical position while promoting a more equitable and secure global future.

Divya Ramjee is an assistant professor, and director of the Technology & Policy Lab, at the Rochester Institute of Technology. She is also an adjunct fellow (non-resident) at the Center for Strategic and International Studies. Dr. Ramjee's research focuses on security, privacy, and policy issues related to cybersecurity, cryptocurrency and blockchain analytics, and AI and other emerging technologies. She has previously worked at various federal government agencies including the Executive Office of the President of the United States, the U.S. Consumer Product Safety Commission, and, most recently, the Computer Crime and Intellectual Property Section at the U.S. Department of Justice.

Evan Selinger is a Professor of Philosophy at Rochester Institute of Technology, where, among other courses, he teaches the Ethics of AI for the graduate AI program. His extensive research focuses on the ethics of technology and includes three books published by Cambridge University Press: "Move Slow and Upgrade," "Re-Engineering Humanity," and "The Cambridge Handbook of Consumer Privacy." Committed to public engagement and public service, he is a contributing writer at The Boston Globe, a frequent contributor to the LA Review of Books, and a member of the Institute for Defense Analysis's Ethical, Legal, and Social/Societal Working Group.

Endnotes

1 Nilsson, N.J. (1971). Problem-solving Methods in Artificial Intelligence. New York: McGraw-Hill.

2 Davenport, T.H. (2018). The AI Advantage: How to Put the Artificial Intelligence Revolution to Work. MIT Press.

3 Ongsulee, P. (2017). Artificial intelligence, machine learning, and deep learning. 2017 15th International Conference on ICT and Knowledge Engineering. https://doi.org/10.1109/ICTKE.2017.8259629

4 Ongsulee, P. (2017). Artificial intelligence, machine learning, and deep learning. 2017 15th International Conference on ICT and Knowledge Engineering. https://doi.org/10.1109/ICTKE.2017.8259629

5 Zewe, A. (2023, November 9). Explained: Generative AI. MIT News. https://news.mit.edu/2023/explained-generative-ai-1109

6 Christensen, C.M., Raynor, M.E., & McDonald, R. (2015). What Is Disruptive Innovation? Harvard Business Review. https://hbr.org/2015/12/what-is-disruptive-innovation

7 Zewe, A. (2023, November 9). Explained: Generative AI. MIT News. https://news.mit.edu/2023/explained-generative-ai-1109

8 Goertzel, B. (2014). Artificial General Intelligence: Concept, State of the Art, and Future Prospects. Journal of Artificial General Intelligence, 5(1), 1-46. https://doi.org/10.2478/jagi-2014-0001

9 Fried, I. (2025, February 6). Exclusive: White House seeks public input on AI strategy. Axios. https://www.axios.com/2025/02/06/trump-white-house-ai-action-plan

10 Exec. Order No. 14110, 3 C.F.R. 75191-75226 (2023). https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

11 Republican Party. (2024, July 8). 2024 GOP Platform: Make America Great Again!. https://rncplatform.donaldjtrump.com/?_ga=2.255281992.1180040526.1729587267-1531562902.1729587267

12 Statistia. (2024). Artificial Intelligence – Worldwide. https://www.statista.com/outlook/tmo/artificial-intelligence/worldwide

13 Szkutak, R. (2024, December 20). Here's the full list of 49 US AI startups that have raised $100M or more in 2024. TechCrunch. https://techcrunch.com/2024/12/20/heres-the-full-list-of-49-us-ai-startups-that-have-raised-100m-or-more-in-2024/

14 Biden White House. (2023, September 12). Biden-Harris Administration Secures Voluntary Commitments from Eight Additional Artificial Intelligence Companies to Manage the Risks Posed by AI [Fact sheet]. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

15 Alder, M. (2024, December 23). Trump taps Michael Kratsios, Lynne Parker for tech and science roles. Fedscoop. https://fedscoop.com/trump-taps-michael-kratsios-lynne-parker-tech-science-roles/

16 Mervis, J. (2024, December 23). Trump names OSTP director as part of White House tech team. Science Insider. https://www.science.org/content/article/trump-names-ostp-director-part-white-house-tech-team

17 Exec. Order No. 13960, 3 C.F.R. 78939-78943 (2020). https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government

18 Exec. Order No. 13960, 3 C.F.R. 78939-78943 (2020). https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government

19 Quotes from US Vice President JD Vance's AI speech in Paris. (2025, February 11). Reuters. https://www.reuters.com/technology/quotes-us-vice-president-jd-vances-ai-speech-paris-2025-02-11/

20 Xi hosts summit with Jack Ma, Chinese private sector leaders. (2025, February 17). Fortune. https://fortune.com/asia/2025/02/17/xi-jinping-jack-ma-summit-meituan-huawei-xiaomi/

21 Office of the Director of National Intelligence. (2024). Annual Threat Assessment of the U.S. Intelligence Community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

22 Metz, C. (2025, January 29). OpenAI Says DeepSeek May Have Improperly Harvested Its Data. The New York Times. https://www.nytimes.com/2025/01/29/technology/openai-deepseek-data-harvest.html

23 Davalos, J. (2025, January 28). DeepSeek Leaned on OpenAI Models, White House AI Czar Sacks Says. Bloomberg Law. https://news.bloomberglaw.com/ip-law/ai-czar-sacks-says-evidence-deepseek-leaned-on-openais-models

24 Trump White House. (2020). National Strategy for Critical and Emerging Technologies. https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf

25 Foundation models are types of generative AI models that use complex neural networks, like generative adversarial networks (GANs). These models are prohibitively expensive and result in large companies focusing on adapting, i.e. "fine tuning," their existing foundation model than creating new ones.

26 Huge "foundation models" are turbo-charging AI progress. (2022, June 11). The Economist. https://www.economist.com/interactive/briefing/2022/06/11/huge-foundation-models-are-turbo-charging-ai-progress

27 Carlini, N., Ippolito, D., Jagielski, M., Lee, K., Tramer, F., & Zhang, C. (2023). Quantifying Memorization Across Neural Language Models. ICLR 2023. https://arxiv.org/pdf/2202.07646

28 National Institute of Standards and Technology. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. Journal of Research of the National Institutes of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

29 Staab, R., Vero, M., Balunovic, M., & Vechev, M. (2024). Beyond Memorization: Violating Privacy Via Inferene with Large Language Models. ICLR 2024. https://arxiv.org/pdf/2310.07298

30 National Institute of Standards and Technology. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. Journal of Research of the National Institutes of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

31 National Institute of Standards and Technology. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. Journal of Research of the National Institutes of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

32 Kibby, C. (2025, February 24). US State Privacy Legislation Tracker. International Association of Privacy Professionals. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

33 Allyn, B. (2024, September 29). California Gov. Newsom vetoes AI safety bill that divided Silicon Valley. NPR. https://www.npr.org/2024/09/20/nx-s1-5119792/newsom-ai-bill-california-sb1047-tech

34 Jenkins, A. (2024, October 29). Texas lawmaker unveils sweeping AI bill for 2025. Pluribus News. https://pluribusnews.com/news-and-events/texas-lawmaker-unveils-sweeping-ai-bill-for-2025/

35 T.X. H.B. 1709, 89th Legislature 2025-2026 (2024). https://s3.documentcloud.org/documents/25257148/texas-responsible-ai-governance-act-traiga-1.pdf

36 Golle, P. (2006). Revisiting the uniqueness of simple demographics in the US population. 5th ACM on Privacy in Electronic Society. https://crypto.stanford.edu/~pgolle/papers/census.pdf

37 L. Sweeney, Uniqueness of Simple Demographics in the U.S. Population, LIDAPWP4. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA, 2000.

38 Gewirtz, D. (2023, January 31). Unlock your trapped data: Driving insights from edge-to-cloud. ZDNET. https://www.zdnet.com/article/unlock-your-trapped-data-driving-insights-from-edge-to-cloud/

39 Gewirtz, D. (2024, December 13). Secret Agentspace: Google announces new AI tool to help enterprises turn silos into lakes. ZDNET. https://www.zdnet.com/article/secret-agentspace-google-announces-new-ai-tool-to-help-enterprises-turn-silos-into-lakes/

40 National Institute of Standards and Technology. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. Journal of Research of the National Institutes of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

41 Menn, J. (2024, August 27). Chinese government hackers penetrate U.S. internet providers to spr. The Washington Post. https://www.washingtonpost.com/technology/2024/08/27/chinese-government-hackers-penetrate-us-internet-providers-spy/

42 Office of the Director of National Intelligence. (2024). Annual Threat Assessment of the U.S. Intelligence Community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

43 Pugh, B., & Harrell, B. (2024, December 23). Feds lay blame while Chinese telecom attack continues. Cyberscoop. https://cyberscoop.com/us-telecom-infrastructure-chinese-cyberattack-salt-typhoon-security-strategy/

44 Borges, C. (2024, May 16). Intellectual Property Rights in the U.S.-China Innovation Competition. Center for Strategic & International Studies. https://www.csis.org/analysis/intellectual-property-rights-us-china-innovation-competition

45 Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 28 C.F.R. § 202-210 (2025). https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern#h-15

46 Exec. Order No. 14117, 3 C.F.R. 15421-15430 (2024). https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related

47 Federal Trade Commission. (2024, September 25). FTC Announces Crackdown on Deceptive AI Claims and Schemes [Press release]. https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

48 Text - H.R.2471 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2022. (2022, March 15). https://www.congress.gov/bill/117th-congress/house-bill/2471/text

49 Department of Defense Chief Information Officer. (n.d.). About CMMC. https://dodcio.defense.gov/cmmc/About/

50 Fjeld, C., Hecht, A., & Sokler, B. (2024, December 20). Congress Passes Defense Bill with AI Provisions – AI: The Washington Post. JDSUPRA. https://www.jdsupra.com/legalnews/congress-passes-defense-bill-with-ai-5565009/

51 Amending and Clarifying Foreign Agents Registration Act Regulations, 28 C.F.R. § 5 (2025), https://www.federalregister.gov/documents/2025/01/02/2024-30871/amending-and-clarifying-foreign-agents-registration-act-regulations

52 Anello, R. (2024, September 11). Unregistered Secret Agents – Annd Multinational Companies – Beware. Forbes. https://www.forbes.com/sites/insider/2024/09/11/fara-unregistered-secret-agents-and-multinational-companies-beware/

53 Office of the Attorney General. (2025, February 5). General Policy Regarding Charging, Plea Negotiations, and Sentencing [Memo]. https://www.justice.gov/ag/media/1388541/dl?inline

54 Fjeld, C., Hecht, A., & Sokler, B. (2024, December 20). Congress Passes Defense Bill with AI Provisions – AI: The Washington Post. JDSUPRA. https://www.jdsupra.com/legalnews/congress-passes-defense-bill-with-ai-5565009/

55 Wilkins, T., & Tucker, C. (2024, December 17). How DC schools are teching teens about online misinformation. NBC Washington. https://www.nbcwashington.com/investigations/how-dc-schools-are-teaching-teens-about-online-misinformation/3794383/

56 Shepardson, D. (2025, March 5). Trump wants to kill $52.7 billion semiconductor chips subsidy law. Reuters. https://www.reuters.com/technology/trump-wants-kill-527-billion-semiconductor-chips-subsidy-law-2025-03-05/

57 Hawkins, M. (2025, March 7). What's at Stake as Trump Looks to Scrap the Chips Act. Bloomberg. https://www.bloomberg.com/news/articles/2025-03-07/what-is-the-chips-act-why-does-trump-want-to-end-it

58 U.S. Economic Development Administration. (n.d.). Regional Technology Innovation Hubs (Tech Hubs). EDA. https://www.eda.gov/funding/programs/regional-technology-and-innovation-hubs

59 https://www.scmp.com/news/china/science/article/3277015/how-chinese-engineers-helped-build-us-semiconductor-empire-timeline

60 Valverde, J. (2024, December 24). China's gallium and germanium bans hit their trade war mark. Asia Times. https://asiatimes.com/2024/12/chinas-gallium-and-germanium-bans-hit-their-trade-war-mark/

61 National Telecommunications and Information Administration. (2024, July 30). Dual-Use Foundation Models with Widely Available Model Weights Report. https://www.ntia.gov/programs-and-initiatives/artificial-intelligence/open-model-weights-report

62 https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/open-weights-foundation-models

63 U.S. Department of State. (2023, November 14). Sunnylands Statement on Enhancing Cooperation to Address the Climate Crisis [Press release]. https://2021-2025.state.gov/sunnylands-statement-on-enhancing-cooperation-to-address-the-climate-crisis/

64 U.S. Economic Development Administration. (2023, October 25). Fact Sheet: Phase 1 Portfolio. https://www.eda.gov/sites/default/files/2023-10/EDA_TECH_HUBS_Phase_1_Fact_Sheet.pdf

65 U.S. Department of State. (2023, November 14). Sunnylands Statement on Enhancing Cooperation to Address the Climate Crisis [Press release]. https://2021-2025.state.gov/sunnylands-statement-on-enhancing-cooperation-to-address-the-climate-crisis/

66 Tison, R. (2024, August 27). Sage Geosystems to build new geothermal project to power Meta data centers. Texas Geothermal Energy Alliance. https://www.txgea.org/sage-geosystems-to-build-new-geothermal-project-to-power-meta-data-centers/

67 Mandler, C. (2024, September 20). Three Mile Island nuclear plant will reopen to power Microsoft data centers. NPR. https://www.npr.org/2024/09/20/nx-s1-5120581/three-mile-island-nuclear-power-plant-microsoft-ai

68 Moseman, A. (2024, August 12). Amazon Vies for Nuclear-Powered Data Center. IEEE Spectrum. https://spectrum.ieee.org/amazon-data-center-nuclear-power

69 Murphy, H., & Criddle, C. (2024, November 4). Meta's plan for nuclear-powered AI data centre thwarted by rare bees. Financial Times. https://www.ft.com/content/ed602e09-6c40-4979-aff9-7453ee28406a

70 U.S. Artificial Intelligence Safety Institute. (n.d.). Home. National Institute of Standards and Technology. https://www.nist.gov/aisi

71 Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, Shmargaret. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? FAccT 2021. https://dl.acm.org/doi/pdf/10.1145/3442188.3445922

72 Greenblatt, R., Denison, C., Wright, B., Roger, F., MacDiarmid, M., Marks, S., Treutlein, J., Belonax, T., Chen, J., Duvenaud, D., Khan, A., Michael, J., Mindermann, S., Perez, E., Petrini, L., Uesato, J., Kaplan, J., Shlegeris, B., Bowman, S. R., & Hubinger, E. (2024). Alignment Faking in Large Language Models [White paper]. Anthropic. https://assets.anthropic.com/m/983c85a201a962f/original/Alignment-Faking-in-Large-Language-Models-full-paper.pdf

73 Rogers, R., and Turk, V. (2025, March 23.) OpenAI's Sora Is Plagued by Sexist, Racist, and Ableist Biases. Wired. https://www.wired.com/story/openai-sora-video-generator-bias/

74 Hagendorff, T. (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. Minds and Machines, 30(1), 99-120. https://doi.org/10.1007/s11023-020-09517-8

75 Von Braun, J., S Archer, M., Reichberg, G. M., & Sánchez Sorondo, M. (2021). Robotics, AI, and humanity: science, ethics, and policy (p. 289). Springer Nature.

76 Lee, N.T., Resnick, P., & Barton, G. (2019, May 22). Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms. Brookings Institution. https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

77 Khorramrouz, A., Dutta, S., Dutta, A., & KhudaBukhsh, A.R. (2023). Down the toxicity rabbit hole: Investigating PaLM 2 guardrails. arXiv preprint. https://arxiv.org/abs/2309.06415v3

78 Oxford Internet Institute. (n.d.). Computational Propaganda. University of Oxford. https://www.oii.ox.ac.uk/research/projects/computational-propaganda/

79 Myers, S. L., & Mozur, P. (2019, August 13). China Is Waging a Disinformation War Aainst Hong Kong Protesters. The New York Times. https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html

80 Bond, S. (2023, August 29). Meta says Chinese, Russian influence operations are among the biggest it's taken down. NPR. https://www.npr.org/2023/08/29/1196117574/meta-says-chinese-russian-influence-operations-are-among-the-biggest-its-taken-d

81 Global Engagement Center. (2023). How the People's Republic of China Seeks to Reshape the Global Information Environment. U.S. Department of State. https://www.state.gov/wp-content/uploads/2023/09/HOW-THE-PEOPLES-REPUBLIC-OF-CHINA-SEEKS-TO-RESHAPE-THE-GLOBAL-INFORMATION-ENVIRONMENT_Final.pdf

82 Wintour, P. (2023, February 28). China spends billions on pro-Russia disinformation, US special envoy says. The Guardian. https://www.theguardian.com/world/2023/feb/28/china-spends-billions-on-pro-russia-disinformation-us-special-envoy-says

83 Cook, S. (2020). Beijing's Global Megaphone: The expansion of Chinese Community Party media influence since 2017. Freedom House. https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone

84 Tartar, A., Rojanasakul, M., & Diamond, J. S. (2018, April 23). How China Is Buying Its Way Into Europe. Bloomberg. https://www.bloomberg.com/graphics/2018-china-business-in-europe/

85 Hader, T., Jensen, B., & Ramjee, D. (2025) [Forthcoming]. How China is Shaping the Indo-Pacific. Center for Strategic and International Studies.

86 Office of the Director of National Intelligence. (2024). Annual Threat Assessment of the U.S. Intelligence Community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

87 Ahn, Y., Lee, S., Shim, J., & Park, J. (2022). Retrieval-Augmented Response Generation for Knowledge-Grounded Conversation in the Wild. IEEE, 10(1). https://doi.org/10.1109/access.2022.3228964

88 Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., Kuttler, H., Lewis, M., Yih, W., Rocktaschel, T., Riedel, S., & Kiela, D. (2020). Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks. 34th Conference on Neural Information Processing Systems. https://arxiv.org/abs/2005.11401

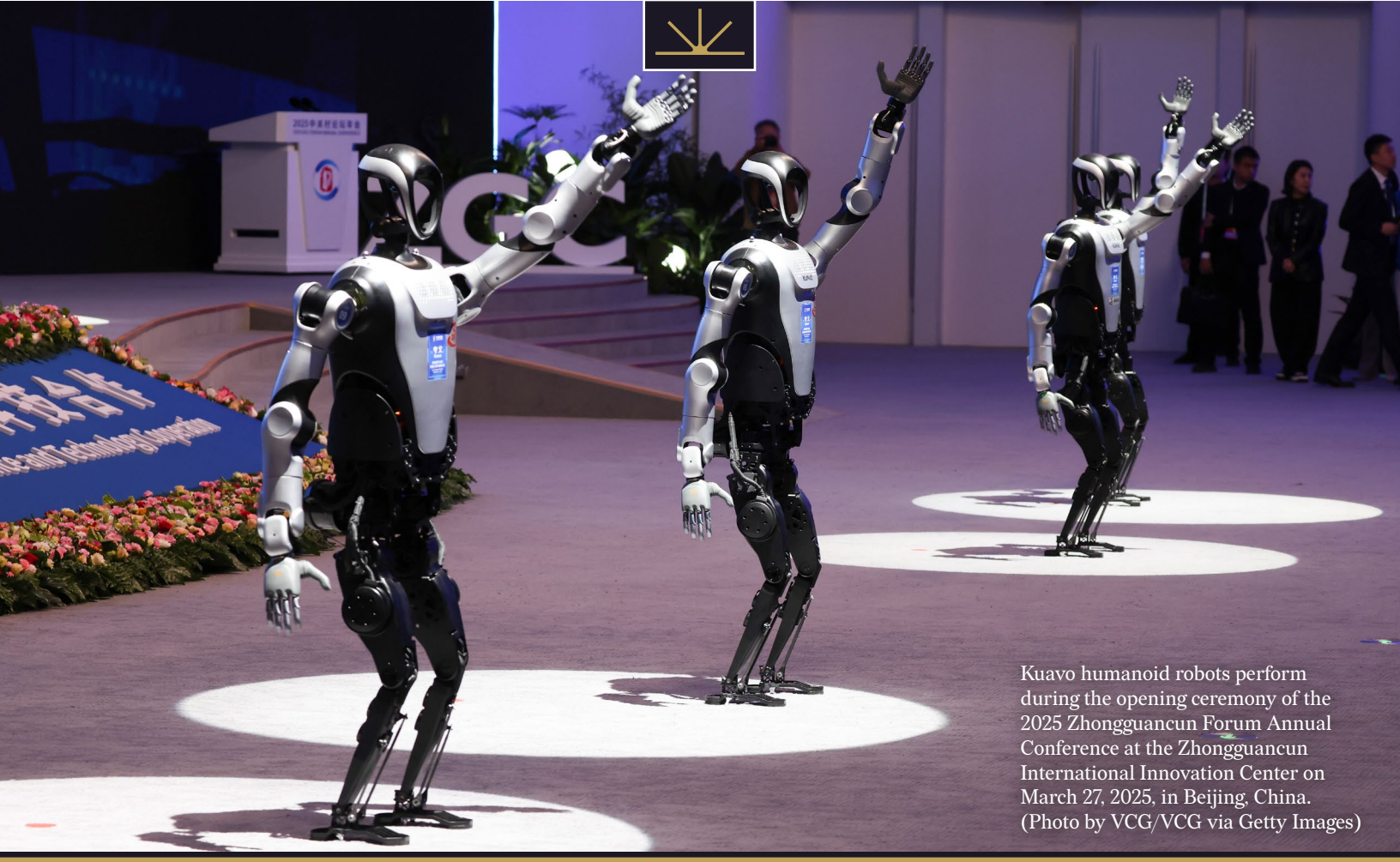
89 Siriwardhana, S., Weerasekera, R., Wen, E., Kaluarachchi, T., Rana, R., & Nanayakkara, S. (2023). Improving the Domain Adaptation of Retrieval Augmented Generation (RAG) Models for Open Domain Question Answering. Transactions of the Association for Computational Linguistics, 11(1), 1-17. https://doi.org/10.1162/tacl_a_00530

90 Bontridder, N., & Poullet, Y. (2021). The role of artificial intelligence in disinformation. Data & Policy, 3, e32. https://doi.org/10.1017/dap.2021.20

91 Humprecht, E. (2018). Where 'fake news' flourishes: a comparison across four Western democracies. Information, Communication & Society, 22(13), 1973-1988. https://doi.org/10.1080/1369118x.2018.1474241

92 Krafft, P. M., & Donovan, J. (2020). Disinformation by Design: The Use of Evidence Collages and Platform Filtering in a Media Manipulation Campaign. Political Communication, 37(2), 194-214. https://doi.org/10.1080/10584609.2019.1686094

93 Blanchette, J., Kennedy, S., Livingston, S., & Glaser, B. S. (2021, January 27). Protecting Democracy in an Age of Disinformation: Lessons from Taiwan. Center for Strategic & International Studies. https://www.csis.org/analysis/protecting-democracy-age-disinformation-lessons-taiwan



Kuavo humanoid robots perform during the opening ceremony of the 2025 Zhongguancun Forum Annual Conference at the Zhongguancun International Innovation Center on March 27, 2025, in Beijing, China. (Photo by VCG/VCG via Getty Images)

American AI Leadership Should Not Be Defined By Machine Learning

Vincent Carchidi

Introduction

U.S. leadership in the development of artificial intelligence should not be defined just by machine learning. This paradigm, in which artificial neural networks learn via data, is a critical step in the progression of this technology. Yet, machine learning is one fundamentally limited paradigm whose shortcomings cannot be overcome by doubling down on its incumbent techniques. U.S. policymakers should instead reconceive of American AI leadership as investing in and pushing the boundaries of the next dominant paradigm in AI. Neuro-symbolic AI,[1] an emerging paradigm that synthesizes techniques from traditional and contemporary approaches to AI research, is the ideal candidate in this respect. It demonstrates the most promising path to ameliorating shortcomings in state-of-the-art models without sacrificing what came before.

However, U.S. officials increasingly define AI leadership in reference to the material needs of machine learning, namely data, computing power, and energy. In July 2024, then-U.S. Secretary of Commerce Gina Raimondo claimed the superiority of American firms' AI models "wouldn't be the case" were U.S. export controls limiting shipments of

advanced semiconductors to China not in place.[2] Her claim implies that the linchpin of American firms' AI leadership is the relative accessibility of computing power.[3]

Raimondo's remark reflects a now-common understanding among policymakers: The path to advanced AI systems is through scale. Scaling up the sizes of models and their training datasets – and then shifting the "scaling up" burden to the time during which models generate outputs – achieves capabilities once the exclusive preserve of human beings. Securing the necessary computing power[4] and energy[5] to train these models is merely the cost of entry, itself the gateway to the "Deep Learning Revolution,"[6] culminating in generative AI.[7] So ingrained is this understanding that the U.S.-China Economic and Security Review Commission's 2024 report recommends establishing a Manhattan Project-like program for "artificial general intelligence" (AGI), complete with executive branch authority to fund multiyear contracts with AI, cloud, and data center firms.[8] This is echoed in analyst recommendations to establish a national computational reserve[9] and to create an AGI commission that helps businesses access data, energy, and computing resources.[10]

This is not the first time that the U.S. government and the AI industry have faced what appears to be the threshold of intelligent machinery. In the early 1980s, the AI systems that captured imaginations were not neural networks but expert systems underpinned by symbolic AI. Their seemingly inexorable rise propelled the Defense Advanced Research Projects Agency (DARPA) to establish the Strategic Computing Initiative in 1983,[11] backed by the U.S. Congress, with the goal of creating a generic expert system capable of underpinning multiple defense applications. While progress in narrow applications was made, the dream of a general system was never realized.[12]

A perceived inevitability accompanies machine learning today. Yet, policymakers have the advantage of hindsight, and with it, a picture of AI's history crystallizes: Advancements made with a new or newly accessible technique in certain areas leads decision-makers to quickly perceive that the achievement of human-level intelligence through this technique is merely a matter of time, only to later realize that the reality of progress in intelligent machinery is never quite as good as it seems.[13]

Policymaking efforts to retain and expand American AI leadership should not concede the future of this technology merely to control its present because its present is fundamentally limited. Machine learning is not the paradigm that will, once fully realized, secure for the U.S. an enduring leadership position in AI. A new paradigm is needed: neuro-symbolic AI. Rather than repeat the mistakes of the past, the U.S. government's role should be relatively targeted and complementary, prioritizing shortcomings in state-of-the-art machine learning systems ripe for improvement in the next paradigm. Rather than pursue AGI, the federal government should invest in frontier neuro-symbolic AI research by laying its foundations through existing offices and programs like the National Artificial Intelligence Initiative Office (NAIIO) and the National Science Foundation's (NSF) National AI Research Institutes.

To make this case, policymakers must understand not only what is happening within the AI industry but what has happened. To that end, a mixed historical, technical, and geopolitical – but accessible – analysis of AI's evolution is provided.

Now is the time to make this argument, as the generative AI boom accounted for over one-quarter of global AI-related private investments in 2023,[14] with U.S. private AI-related investment coming in at a world-leading $67.2 billion in 2023 (compared to China at $7.8 billion).[15] It also comes as U.S. federal funding for AI research and development has more than tripled since fiscal year 2018, with government agencies allocating a total of $1.8 billion in 2023.[16] The highest AI R&D agency requests for FY 2024 came from the NSF ($531 million), DARPA ($322.1 million), and the National Institutes of Health (NIH) ($284.5 million).[17]

Four recommendations are provided, implicating both the U.S. Congress and the Executive Branch:

1. The NAIIO should direct the federal AI Research & Development Interagency Working Group to prioritize long-term investments in neuro-symbolic AI as part of its mandate to promote U.S. AI leadership.

The Godfather of AI' Geoffrey Hinton, speaks at 'Can we control AI?' panel during day two of Collision 2024 in Toronto, Ontario, on June 19, 2024. (Mert Alper Dervis / Anadolu via Getty Images)

2. The NSF should expand its network of National AI Research Institutes by establishing an Institute dedicated to foundational and use-inspired neuro-symbolic AI research in a critical sector, complete with corporate and academic public-private partnerships.
3. Congress should fulfill the promise of the CHIPS and Science Act by increasing federal agencies' basic research budgets.
4. Congress and the Commerce Department should adopt proactive yet targeted export controls on hardware and models in coordination with partners and allies that are proportional to the capabilities of AI models.

The First Two Waves of AI

Fortunately, DARPA adopted a useful conceptualization [18] of AI's technical trajectory to guide understanding of this technology's development, dividing it into three stages: First Wave; Second Wave; and an anticipated Third Wave that ameliorates the shortcomings of the first two.[19] The First Wave was dominated by symbolic AI, characterized by systems built with human knowledge encoded directly into the systems. The current Second Wave is dominated by machine learning, in which neural networks learn via data.

A historical analysis reveals not only what went wrong in the First Wave but why it went wrong. Concomitantly, it shows us how critical the U.S. government's support for basic AI research was before the ascendence of symbolic-based expert systems led to over-promise and under-delivery. The lessons of this history bear directly on the U.S. government's role in the Third Wave.

Foundations of the First Wave

The U.S. government's role in supporting AI as it grew from a collection of scattered research efforts to a recognizable discipline is critical and often overlooked. Although AI originated in the private sector, its early growth was principally dependent on public investments in fundamental research programs. ARPA (later rebranded DARPA) was disproportionately responsible for this transformation through the 1960s to the 1990s, with the initial 10-15 years of AI funding enabling basic and interdisciplinary research without concern for immediate applications. Over time, additional major sources of federal support included other Department of Defense agencies, NIH, NSF, and NASA.[20]

Early pioneers in AI included mathematician Claude Shannon, computer scientist John McCarthy, and then-graduate student Marvin Minsky, who was recruited to work with Shannon and McCarthy at Bell Laboratories. IBM's Nathaniel Rochester shared their belief that AI showed significant promise, with Rochester joining the 1956 Dartmouth workshop on AI.[21] The workshop's associated research proposal[22] is considered a founding document in AI, with all four individuals as coauthors.

That same year, the U.S. Air Force (through Project RAND) funded nearly the entirety of Herbert Simon and Allen Newell's work on Logic Theorist, a computer program that could prove select mathematical theorems. Newell went to work at Carnegie Tech (now Carnegie Mellon University), where the Air Force and Office of Naval Research largely funded the projects on decision-making and problem-solving

until the early 1960s. At the Massachusetts Institute of Technology, Minsky and McCarthy established the Artificial Intelligence Project in 1957. Here too, military funding was critical, though informally leveraged through an arrangement with the Research Laboratory of Electronics.[23]

Moreover, ARPA's Information Processing Techniques Office (IPTO) increased funding for Stanford University in 1965 to upgrade computing capabilities, following McCarthy's establishment of the Stanford Artificial Intelligence Laboratory in 1963.[24] Stanford Research Institute's Artificial Intelligence Center, founded in 1966, worked on automatons that could gather, process, and transmit data in a hostile environment, leading to the AI-enabled robot "Shakey," whose construction required basic research in planning, natural language processing, and computer vision. Funders, however, were not satisfied despite progress,[25] foreshadowing the field's perennial discontents.

Such discontents were magnified by external scrutiny in the mid-1970s, leading DARPA Director George Heilmeier (taking office in 1975) to cut the agency's speech understanding research and become more insistent that AI research be linked to mission-oriented applications.[26]

The First Wave's Zenith: Symbolic AI

Throughout this period, artificial neural networks (ANNs) existed, but they were overshadowed by the approach that dominated the First Wave: symbolic AI.[27] Symbolic systems are hand-coded with human knowledge. Think of this feature of symbolic systems as their defining characteristic, separating them from other types of AI. These systems represent human-defined knowledge using symbols, such as words, rules, or formal logic. They do not learn this knowledge from data. The system manipulates these symbols to ascertain relationships between them via the rules or logical statements with which it is innately endowed. Symbolic AI systems thus produce human-interpretable results.[28]

The premise of symbolic AI was simple: once a machine is given sufficient structured facts about the world (handcrafted knowledge), dynamic intelligence will eventually result. Too simple, in fact, as this approach – while finding some successes in expert systems – crashed in the late-1980s as cheap, accessible computers supplanted symbolic-based expert systems that required specialized hardware.[29]

In the late-1970s, however, momentum was shifting towards expert systems. IPTO Director Robert Kahn, who took office in 1979, broke with Heilmeier in seeing real-world promise for them. Simultaneously, there was increasing congressional concern about the threat posed by the Japanese Fifth Generation Computer Systems program to U.S. technological leadership.[30] The result was the establishment of DARPA's Strategic Computing program.

Kahn sold his vision to Congress through the promise of specific AI-enabled applications. Interestingly, the Japanese program powerfully influenced congressional deliberation over Kahn's requests. This partly owed to the publication of computer scientists Edward Feigenbaum and Pamela McCorduck's book "The Fifth Generation,"[31] in which they call on the U.S. government to meet the Japanese challenge. They invoked the idea, as Colin Garvey summarizes, that "expert systems were transforming computers from "calculating machines" that relied on data, to "reasoning machines" that relied on knowledge."[32] Congress approved Kahn's plan by splitting Strategic Computing into two major projects: one for specific applications and another for basic research in support of those applications.[33]

Research in areas like speech understanding that had previously been cut resumed on a large scale in 1984 and persisted into the 1990s with participation from private actors including Carnegie Mellon, MIT, and IBM. DARPA sought to mutually hammer out performance evaluation benchmarks between DARPA managers and funded researchers.[34] DARPA and the National Bureau of Standards (now the National Institute of Standards and Technology (NIST)) held annual system evaluations with government contractor, industry, and university participation. This enhanced rates of adoption and commercialization, though it may have moved away from basic research, as the increased adoption simultaneously lowered the need for basic research.[35]

Unfortunately, early optimism in the potential of expert systems was unwarranted. The Strategic Computing program's founders disagreed on how to best direct its research projects. As Emma Salisbury details, the division was between Kahn, who believed that applications would flow naturally from a developed technology base, and DARPA Director Robert Cooper, who believed that specific applications would give way to a more developed technology base.[36]

This division foreshadowed the downfall of Strategic Computing. By 1988, the program's ambitions were downgraded. By 1993, it was a memory. As Salisbury observed, it is not surprising that an initiative of such interdependent ambition failed. While it did produce successes in computer vision, natural language understanding, and speech recognition, the program failed, she argues, because of overpromise and underdelivery. Indeed, the unusual structure of the program positioned it for this outcome: It funded not only specific research problems but also a multifront, field-wide agenda in which progress in one area was expected to aid the progress of another. This, in turn, was enabled by the founders' willingness to see general AI as a realistic possibility through advancements in computing power.[37]

The Second Wave (Approx. 2012 – present)

The First Wave did not see enduring success. Handcrafted knowledge was not sufficient for the lofty goals of AI, and symbolic AI fell out of favor. The fall of Strategic Computing and the disappointment of expert systems exemplify a familiar boom-and-bust cycle in AI's history, which reverberates in the Second Wave.

The Second Wave eschews the First Wave's reliance on handcrafted knowledge. Instead, it promotes ANNs that learn via statistical associations of data. The ability to learn via data is what separates ANNs from symbolic systems.

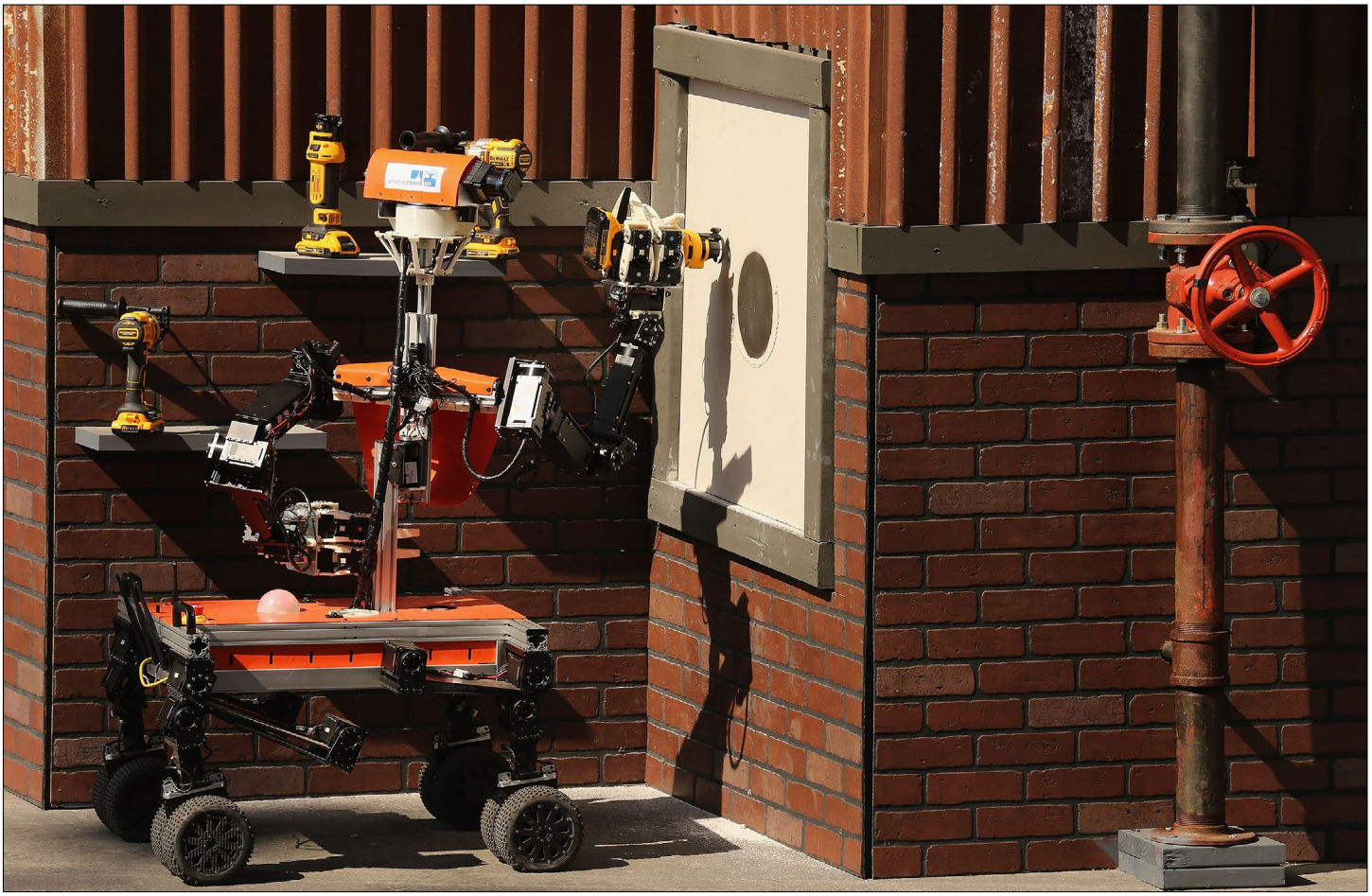
This approach is known as machine learning. Its premise is that the assemblies of neurons in biological brains, with all their marvelous interactivity, can be replicated through these artificial networks. A neural network generates predictions about a given task (e.g., predicting the next word, predicting the type of object in an image, etc.). Since the network is not generating these predictions by manipulating human-defined symbols, their predictions are based on their training data. ANNs learn when a word is used or what an object looks like based on that word's or object's distribution in their training data.

Early ANNs were shallow, consisting of a single layer of neurons between input and output. Deep learning simply refers to later ANNs that contain many layers of neurons. Even here, the U.S. government's footprint is visible. One of the first practical instantiations of ANNs – Frank Rosenblatt's Mark I Perceptron[38] – resulted from image recognition work[39] funded by U.S. defense agencies amid broader efforts to develop automatic target recognition.[40] Deep learning pioneer and Nobel laureate Geoffrey Hinton[41] was also supported by NSF funding in the 1980s.[42]

Nevertheless, the U.S. government's role in the Second Wave is markedly different than its role in the First Wave. It is a cliché that machine learning blossomed in the private sector.[43] Companies like Google, DeepMind, OpenAI, Microsoft, and Meta are responsible for the most recent innovations. Indeed, the U.S. government's distanced role in the Second Wave reflects a broader trend. Zegart details how the peak of federal funding for research generally as a share of GDP came in 1964, when it was at 1.9%. By 2020, it had fallen to 0.7%. Basic research funding through major sponsors like the NIH and NSF has struggled, particularly as the latter's budget was cut by 8% in 2024. The 2022 CHIPS and Science Act,[44] which was designed in part to revitalize American basic research, was unable to fill the gaps.[45]

The mismatch between the priority that U.S. policymakers now place on U.S. AI leadership and funding allocations to federal agencies is a disjuncture from AI's First Wave.

That said, one program is particularly important for the U.S. government's role in AI research today: the NSF's National AI Research Institutes.[46] Program Lead James Donlon explained that this relatively new program is central to the U.S. government's AI R&D strategy.[47] Crucially, the Institutes adopt a "use-inspired research framework" that seeks solutions for domain-specific applications where current approaches fall short.[48] Institutes are encouraged to plan for long-term,



The Team NimbRo Rescue semi-autonomus robot uses a power tool to cut through drywall during the Defense Advanced Research Projects Agency (DARPA) Robotics Challenge at the Fairplex June 5, 2015 in Pomona, California. (Chip Somodevilla / Getty Images)

interdisciplinary research projects that contribute to the AI objectives in the National AI R&D Strategic Plan.[49] This includes strengthening and expanding public-private partnerships across government agencies, non-governmental organizations, academia, and industry.[50] Institutes also emphasize complementarity: The federal government's role is to take on "high-risk, high-reward projects" while recognizing that the private sector excels in advanced technology offerings, understanding market trends, and providing access to data and computational resources.[51]

The institutes' mandate thus sidesteps the messiness of Strategic Computing's debate by ensuring their domain-specificity and diffusion while also linking basic research with applications where state-of-the-art techniques do not suffice and emphasizing public-private partnerships and complementarity.

The NAIIO, as well as the National Science and Technology Council's Subcommittee on Machine Learning and Artificial Intelligence,[52] oversee the AI R&D Interagency Working Group (IWG).[53] The IWG, for its part, coordinates and supports long-term investments in AI R&D and applications geared toward U.S. leadership and global competitiveness.[54] This, in turn, includes support for the National AI Research Institutes.[55]

The establishment of the AI Research Institutes was mandated by the National Artificial Intelligence Initiative Act of 2020 ,[56] which calls on the NSF to "lead Federal agencies in providing investments to jump-start … innovations through National AI Research Institutes."[57] Indeed, the institutes are the NSF's flagship program for foundational and use-inspired AI research and the largest research ecosystem funded

through partnerships between federal agencies and industry leaders, with $500 billion in total investment across 500 collaborative organizations globally as of 2023[58] and 27 institutes in operation.

Nevertheless, if the disappointments of the First Wave are repeating in the Second, one should be able to trace the fundamental and persistent shortcomings of machine learning through the present day. Indeed, these shortcomings can be identified in fundamental areas including reasoning and planning, abstraction and generalization, factual accuracy, and analytic depth. This undermines AI systems' ability to deliver performance guarantees and provide output of reliability sufficient to justify their critical uses, representing a historical repeat in its own right: In 1984, criticism of Strategic Computing acknowledged the capabilities of AI but cautioned that it "creates a false sense of security" given AI systems' propensity to "act inappropriately in unanticipated situations" owing to a "fundamental limit on their reliability."[59]

Concomitantly, one should be able to detect the U.S. government's role in affirming the perception that intelligence's threshold is being crossed – and one does, particularly in the flow of hardware and export controls therein.

Yet, machine learning's capabilities and limitations are two sides of the same coin; the latter a corollary of the former. Thus, before approaching these limitations, we must understand the Second Wave's deep learning revolution and its intertwining with geopolitics.

The Second Wave's Deep Learning Revolution

The deep learning revolution in part results from the success of a computer vision model[60] known as "AlexNet" in a 2012 image recognition contest.[61] AlexNet outcompeted previous approaches that relied on manually coding features of an image[62] (i.e., symbolic approaches). It instead used the newfound access to vast amounts of data to learn how to discern those features during training. AlexNet marked a break, then, from the First Wave into the Second when "[c]omputation and scale are much more important than human knowledge" in the construction of AI systems.[63] Think of AlexNet as a proof of concept for a realistic alternative to symbolic AI.

During its training, AlexNet performed 4.7×10^{17} floating-point operations – this merely refers to the number of times two numbers are added together or multiplied, though this sheer amount of computation was enormous (roughly four-hundred and seventy quadrillion operations!)[64] Past approaches to image recognition did not tend to be as computationally intensive. Indeed, Central processing units (CPUs) were not up to the task of efficiently handling these operations. Thus, AlexNet was trained using two graphics processing units (GPUs), a specialized chip for high-quality image and video processing. An emphasis, then, on data and specialized hardware was present right from the start.

This revolution seeped into strategic reasoning AI. In 2016, DeepMind's AlphaGo, a Go-playing system, defeated international professional player Lee Sedol in four out of five games,[65] exceeding observer expectations. AlphaGo accomplished this with one foot in symbolic AI and the other in machine learning. It linked a problem-solver search algorithm with two deep neural networks.[66] The beauty lies in the interaction between this search algorithm and the neural nets. The search algorithm branches out in a tree-like formation to simulate possible game moves and pathways. The neural networks increase the efficiency of the search algorithm by guiding it towards higher-probability moves (those moves that one network deemed more likely to be made based on the current board state) and then precisely evaluating moves.

The strength of these networks is how they were trained. Two sources of data were involved. The first was data of Go moves made by human expert players. The other was data produced via self-play; that is, data produced by the networks by playing against copies of themselves. AlphaGo's networks were trained on 50 GPUs for one week and three weeks, respectively.[67] During runtime, a "distributed" version of AlphaGo that leverages multiple machines used 1,202 CPUs and 176 GPUs[68] – an indication that not only does the scale of computation matter but also that specialized hardware is demanded.

The self-play technique, formally known as self-play reinforcement learning, took center-stage in 2017 with DeepMind's AlphaGo Zero. It defeated

Facebook accelerates research efforts in Germany on artificial intelligence and machine learning by presenting at the Axel Springer Award in Berlin on Feb. 25, 2016. (Kay Nietfeld / AFP via Getty Images)

AlphaGo, the system that bested Lee, 100-0 – a stunning improvement.[69]

AlphaGo Zero doubles down on deep learning. Specifically, AlphaGo Zero's architecture was simplified to just a single deep neural network. More than this, the network was trained without using examples of human expert moves. As before, the network was trained through self-play, rewarded for wins and punished for losses. Importantly, AlphaGo Zero still possesses the problem-solving search algorithm. The original interactivity between the search algorithm and the neural network in the predecessor AlphaGo was carried into AlphaGo Zero.[70]

AlphaGo Zero's neural network was trained on both GPUs and CPUs and used specialized processors during runtime designed by Google.[71] The emphases on data and specialized hardware persist.

AlphaGo Zero marks a step change from IBM's 1997 chess-playing Deep Blue, which in part relied on internal knowledge related to positions and lines of attack that were hand-coded directly into the system,[72] and received significant input from human grandmasters.[73] Indeed, the AlphaGo research paper explicitly distinguishes Deep Blue's reliance on handcrafted rules from AlphaGo's learning via data.[74]

The momentum for deep learning is most evident in natural language processing (NLP). Historically, NLP's grand challenges relate to the Turing Test,[75] in which a computer, competing against a flesh-and-blood human, convinces a second human it is a real person through anonymized conversation. The successes of the generative pre-trained transformer (GPT) architecture changed attitudes about natural language conversation with machines, with the transformer invented by Google researchers in 2017.[76] GPTs improved with scale through OpenAI's GPT-2[77] and GPT-3,[78] unveiled in 2019 and 2020, respectively. GPT-3's apparent fluency is reminiscent of machines that could pass the Turing Test.[79]

GPT-3's research paper explicitly emphasizes the importance of increasing the size of the model from

GPT-2 to GPT-3, its training dataset size and diversity, and the length of training,[80] reinforcing the association between the scale of computation and specialized hardware with capabilities.[81]

November 2022's ChatGPT-3.5[82] was built on a modified version of GPT-3. OpenAI released GPT-4[83] in March 2023. The model is widely believed to follow the "scaling up" trend, though OpenAI declined to share technical details.[84] Nonetheless, Epoch AI estimates that computing power for AI training increased by almost eight orders of magnitude between AlexNet and GPT-4.[85] The emphasis on specialized hardware persists into 2025, with major companies planning a combined spend of $320 billion on AI and data center build-outs.[86]

Suffusing Machine Learning and Geopolitics

U.S. policymakers have shown increasing interest in AI throughout its Second Wave as the accomplishments under the deep learning revolution accrue and access to hardware becomes intimately linked with progress. There is a distinction, to be sure, in the scope and urgency of U.S. AI policymaking before and after ChatGPT-3.5, though the policy pathway paralleled the industry's apparent growth before this watershed.

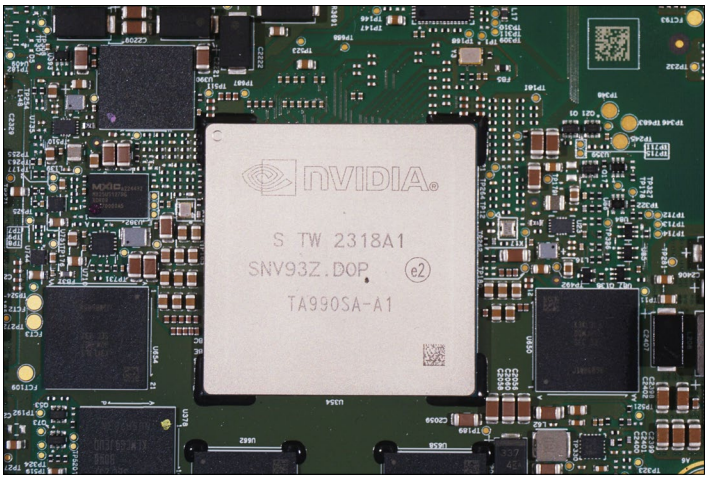
The emphasis that U.S. officials place on restricting the flow of AI-related hardware to China follows the adversaries' great-power competition. The first administration of President Donald Trump oversaw the escalation of a U.S.-China trade dispute that had simmered since the George W. Bush and Barack Obama administrations, intertwining with the Chinese acquisition of sensitive American technologies.[87] U.S. concerns about Chinese access to advanced semiconductors manifested with a pressure campaign on the Dutch government, reported in January 2020,[88] to block sales of chip manufacturing technology to China. The Dutch government decided not to renew the export license for semiconductor equipment maker ASML's extreme ultraviolet lithography (EUV) machine,[89] over which it has supply chain dominance (and depends partly on American technology, giving export controls force.)[90] In May 2020, the first Trump administration amended the Foreign Direct Product Rule (FDPR) to restrict the shipment of semiconductors from global chipmakers to Huawei.[91]

Displaying continuity,[92] in September 2022 the administration of President Joe Biden instructed[93] Nvidia and Advanced Micro Devices (AMD) to cease exporting Nvidia's A100 and H100 chips and AMD's MI250 chips to China – each used in AI development. In October 2022, mere weeks before ChatGPT-3.5 debuted, the Bureau of Industry and Security[94] published an extensive array of export controls designed to restrict Chinese firms from obtaining advanced semiconductors and chipmaking equipment, including a ban on the export of certain chips to China made anywhere in the world with U.S. equipment.[95]

That was pre-ChatGPT. Now, the imperative to gain access to hardware, infrastructure, and energy is more pronounced. [96] In September 2024, BlackRock and Microsoft[97] shared plans to launch a $30 billion private equity fund, dubbed the Global AI Infrastructure Investment Partnership, to build data centers and energy infrastructure to meet AI demand.[98] Abu Dhabi-based MGX, a state-backed AI investment vehicle, is a general partner in the fund alongside Microsoft.[99] Relatedly, in late 2024 Microsoft and Google reached agreements with Constellation Energy and Kairos Power, respectively, to purchase nuclear energy.[100]

As developments unfold, the U.S. has continuously adapted its export controls. The outgoing Biden administration released its "Diffusion" Framework in January 2025.[101] The Framework is comprehensive, dividing the world into three tiers of most to least U.S.-aligned. It also builds on its Data Center Validated End User (VEU) program, allowing companies to apply for National or Universal VEU applications.[102]

Moreover, the U.S. has engaged allies to harmonize restrictions on advanced chips to China. Following the Dutch government's January 2023 restriction on the export of deep ultraviolet lithography machines to China,[103] the Dutch government would, in August 2024, align itself[104] with the U.S. (after some wrangling[105]) by withholding the renewal of ASML's licenses to service and provide spare parts for 1970i and 1980i[106] DUV immersion tools. December 2024's exemption of the Dutch and Japanese, but not states like



An automotive-grade chip developed by NVidia is seen at MWC 2024 in Shanghai, China. (Long Wei / Feature China/ Future Publishing via Getty Images)

South Korea, in its application of the FDPR followed this patchy history.[107]

U.S. officials are highly attuned to the increased demand for advanced chips and infrastructure. OpenAI CEO Sam Altman is trying[108] to persuade officials and investors[109] to pour billions of dollars into AI infrastructure, including financing of new data centers[110] and (at one point[111]) a new chip-building venture,[112] to fuel the large-scale deployment of AI systems. At the White House in September 2024, he pitched the idea that "Infrastructure Is Destiny" and new AI data centers costing $100 billion each should be built – urgently – as a means of reindustrialization.[113]

In November 2024, OpenAI representatives presented a "blueprint for U.S. AI infrastructure" in Washington, D.C, envisioning an infrastructure build-out for AI, complete with state and federal co-created economic zones, a National Transmission Highway Act, and a North American AI Alliance proposal grounded in competition with China.[114] The "Stargate" data center project, jointly announced with Trump in January 2025, might be considered a very partial manifestation of the effort, with government playing a de-regulatory – rather than direct funding – role.[115]

Is Machine Learning the Holy Grail?

A critical mass of American policymakers and officials, then, are locked into the idea that the machine learning paradigm, and more specifically deep learning, is the future of this technology. Retaining American AI leadership – defined by machine learning – thus requires deference to the infrastructural needs of its developmental trajectory; its scaling up. Altman summarizes this sentiment: "In three words: deep learning worked. In 15 words: deep learning worked, got predictably better with scale, and we dedicated increasing resources to it."[116]

This view is seriously problematic, and U.S. policymakers must confront its deficiencies. First, headline-grabbing accomplishments are often more limited than they appear. Second, standards of achievement for AI systems – what counts as a system being "capable" of something – are dramatically lower than in traditional computer science applications. Finally, systems that do merit the descriptor "superhuman" are often more isolated than promoted, not portending future developments that can be seamlessly applied from one domain to another.

What policymakers need today is a view of the machine learning landscape that identifies these shortcomings without dismissing the capabilities this paradigm has achieved (what the architects of Strategic Computing, and their Congressional backers, likewise needed). This requires some level of technical engagement. This is provided below, exploring areas including reasoning and planning, abstraction and generalization, factual accuracy, analytic depth, and intellectual autonomy.

The Misperception of Boundless Innovation

An Arizona State University (ASU) research group led by Subbarao Kambhampati[117] tested the reasoning and planning abilities of large language models (LLMs) from 2022 to 2024, finding that they lag well behind humans: GPT-3 exhibited "dismal performance" when initially tested. [118] A follow-up test found that, while GPT-4 had improved performance over its predecessor by reaching roughly 35% accuracy in a test that requires it to generate plans for stacking blocks ("Blocksworld"),[119] it averages a mere 12% success rate in generating executable plans across domains.[120]

Kambhampati thus likens LLMs' performances to approximate retrieval: LLMs have access to internet-sized datasets, yet unlike a traditional database that faithfully retrieves data exactly as it is stored, LLMs complete an input by reconstructing said data in a probabilistic fashion to generate an output. The ensuing novelty of the output merely looks as though the model is reasoning.[121]

Still, LLMs' purported reasoning abilities often rest on their benchmark scores. Yet, researchers Martha Lewis and Melanie Mitchell highlight the lack of robustness of these scores. They test the analogical reasoning abilities of LLMs – this includes problems that require human and LLM subjects to transfer the abstract structure of one problem to another (e.g., given an original story, participants must judge which of two separate stories are more or equally analogous to the original).[122] When models including GPT-3, GPT-3.5, and GPT-4 are tested on variants of tasks on which LLMs previously performed well – despite their abstract structures remaining the same – LLMs display "brittleness on most of the variation and biases we tested."[123] LLMs' lack of robustness indicates that when LLMs do perform on a par with humans, it is merely because they encountered sufficiently similar problems in their training data, whereas humans appear capable of overcoming their biases through "metacognitive deliberation."[124]

Other problems persist in GPT-based systems. Hallucinations – inaccurate or fictional outputs that LLMs sometimes produce – could be an indefinite problem.[125] Some researchers argue that hallucinations are structural and there is no possibility of ensuring complete accuracy even with access to perfect, up-to-date data.[126] Additionally, even if hallucinations were eliminated, LLMs' responses – particularly in critical applications – still lack sufficient analytical depth.[127]

Would further scaling up – the deep learning revolution's secret ingredient – remedy these flaws? This is unlikely. Research released in April 2024 testing multimodal models – those trained on multiple modalities other than text, like images – finds that the increased performance of the model on a new problem is utterly dependent on how many times the relevant concept appears in its training dataset – and even an exponential increase in training data yields only linear improvements in capabilities.[128] Put simply: More training data may not be enough for the desired capabilities.

Beyond hallucinations, the abstraction and generalization abilities of LLMs are likewise not adequately improved by training on multiple modalities. GPT-4's text-only and multimodal features lack the robust ability to form abstractions relative to humans.[129] On an abstract visual reasoning benchmark, designed with inspiration from human child psychology, multimodal LLMs (including GPT-4V, Claude 3 Opus, Claude 3 Sonnet, and Gemini) give a near-random performance, lagging 40% behind humans.[130]

Finally, testing LLMs on problems related to the pressures of their training environment and its objective – to predict the next word based on the statistical distribution of words in a dataset – find that LLMs' accuracy "can indeed vary substantially" depending on the probability of the example tested.[131] Put simply: LLMs perform better or worse depending on the likelihood of their encountering the type of problem during training, rather than reasoning through them independently.

Unsurprisingly, then, LLM scores on the ARC-AGI-1 Prize[132] – a competition based on the 2019 Abstraction and Reasoning Corpus for Artificial General Intelligence (ARC-AGI) that assessed the capacity for "skill acquisition" and adaptation to a changing environment[133] – are disappointing. On the public, noncompetitive version of ARC-AGI, Claude 3.5 scores 21%, whereas GPT-4o scores 9%.[134]

All this points to fundamental problems in contemporary AI. A paper co-written by Peter Voss, who co-coined the term "AGI,"[135] argues that LLMs are premised on an approach that is fundamentally inconsistent with the original concept of AGI. The focus of the field "shifted from having internal intelligence to utilizing external intelligence (the programmer's intelligence) to solve particular problems."[136] LLMs are woefully unable to autonomously acquire new skills, instead dependent on the instructions, guides, and clues provided by intelligent humans to leverage the resources they possess.

(L-R) Jeff Seibert, Co-founder and CEO of Digits, Kevin Weil, CPO, OpenAI, and Kate Rooney of CNBC speak at the HumanX AI Conference 2025 in Las Vegas, Nevada on March 10, 2025. (Big Event Media / Getty Images for HumanX Conference)

Do OpenAI's 'o1' Models Lay Our Fears to Rest?

To be sure, recent developments ostensibly aim to cure AI's ailments. OpenAI's newest "o1"[137] models are allegedly capable of "reasoning."[138] The company says its o1-preview model performs comparably to doctoral students on benchmark challenges in physics, chemistry, and biology.[139] Both reinforcement learning and "chain-of-thought" (CoT) reasoning are used in o1's design and training.[140] CoT is a technique in which a model is prompted to break down problems into "intermediate natural language reasoning steps that lead to the final output"[141] (i.e., breaking down a problem step-by-step).

OpenAI declined to share architectural details about o1. Plausibly, a modified version of an LLM (e.g., GPT-4o) is pre-trained on data of CoTs; examples of useful reasoning steps expressed via natural language. This model is now capable of predicting the most likely CoT based on the given prompt – think of this as the distribution of CoTs. A reinforcement learning model is then coupled with the modified LLM to hone the distribution of CoTs. Using a specified reward signal (a la AlphaGo Zero), this model generates, selects, and extends a CoT, effectively prompting itself to lengthen the reasoning steps, refining its selection over time.[142]

Whatever the case, when o1 responds to end-users' queries, the response times are unusually lengthy because it is expanding the steps in the "thought process" for improved accuracy. Thus, OpenAI did not move away from the "scaling up" trend but instead applied it to the time during which the model generates outputs.[143]

The reasoning models are both sufficiently different from earlier LLMs to justify a delineation between them and fundamentally deficient in the ways outlined above. The visible throughline is an improvement along some capability measures – say, higher scores on benchmarks – without concomitant improvements in reliability and performance guarantees, factual accuracy, reasoning (names notwithstanding), planning, analytical depth, and so forth.

On a public (non-competitive) version of the ARC-AGI-1 test, o1-mini scored 13% and o1-preview scored 21% (equal to Claude 3.5s, though higher than GPT-4o's 9%).[144] ARC Prize co-founder Mike Knoop explained

that the extended CoT prompting does improve the model's ability to adapt to novelty, though o1-preview's parity with Claude was achieved by taking nearly 10 times longer.[145] (On "o3," see below.)

Furthermore, Apple researchers tested 25 state-of-the-art LLMs, including the o1 models, on their logical reasoning capabilities. The researchers did this cleverly: They took a grade-school mathematics benchmark and generated new variants of its mathematical reasoning problems, allowing the researchers to test LLMs through various setups of the questions (much like Lewis' and Mitchell's tests above). For example, one experiment changed the proper nouns (e.g., names) and the numbers of a problem without changing their actual meanings. Other experiments inserted additional clauses into the problems, some relevant and others irrelevant to their required reasoning steps.[146]

On problems where clauses were inserted to increase the difficulty of the problem, all models exhibited performance decreases and variance increases – accuracy diminished, variability ticked up. The rate at which accuracy dropped increased in tandem with the increasing difficulty of the problem. The models' pattern-matching is simply less robust as difficulty increases.[147] When irrelevant, inconsequential clauses were inserted into problems, all models exhibited "catastrophic performance decline,"[148] indicating that models are reliant on pattern-matching the data on which they have been trained.

Interestingly, this research converges on other work in finding that o1-mini and o1-preview exhibit significant improvements over earlier LLMs, yet retain their fundamental shortcomings. The Apple researchers carefully note that o1-preview is not prone to the same type of performance drop and variance on difficulty increases as o1-mini and other models. Yet, both models show a significant performance drop on those problems where irrelevant clauses are inserted into the problems[149] – indicating a lack of genuine logical reasoning. Similarly, the researchers who found that LLMs' accuracy is susceptible to the probability of a given task found that the o1-preview shows "substantial improvement" over previous LLMs, but it continues to exhibit the "same qualitative behavioral patterns that we observed with other LLMs."[150] As other researchers poignantly note, these so-called foundation models "do remain interestingly fragile, especially to unforeseen situations…"[151]

Similarly, the ASU research group tested o1's ability to plan, showing a marked improvement over past LLMs. Testing on three variants of the Blocksworld test, o1-preview performs exceptionally well on the version with complete knowledge of the problems (97.8% accuracy), less well on a version with incomplete knowledge (52.8% accuracy), and a poorer result on an altered, randomized version of the test (37.3% accuracy). These results blow LLMs like Claude 3.5 Sonnet out of the water.[152]

Yet, the retainment of fundamental limitations continues, this time with a First Wave twist. Contrast o1-preview's performance on Blocksworld with a far cheaper, less computationally intensive symbolic planner. This system, Fast Downward,[153] achieves 100% accuracy on all Blocksworld planning tests – perfect scores across the board. The researchers emphasize that Fast Downward accomplishes this in "a fraction of the time, compute, and cost, while providing guarantees that their answers are correct."[154]

That last part is worth our focus. The deep learning revolution is accompanied by a lower standard of achievement for AI systems; they are often claimed to possess a capability, yet they are unable to guarantee the performance that would be expected of said capability. An LLM "can" provide factual, conversation-like text, but it cannot do so reliably; a "reasoning" model like o1-preview "can" plan but it cannot match the performance of a preceding system – in what sense can both Fast Downward and o1-preview "plan?" Computer science applications are traditionally expected to provide "performance guarantees."[155] Deep learning systems often do not.[156]

The Second Wave's mantra is that models like o1 may lag behind systems like Fast Downward in narrow domains, but these are more general models – capable of more than mere planning. Yet, fundamental shortcomings persist as costs of entry rise. New models do not summarily move in a single direction. Nor do models that achieve new capabilities offer performance guarantees one expects from their

narrower symbolic predecessors or from a system deserving of the name "artificial general intelligence."

Note on Confusion Surrounding OpenAI's "o3"

In December 2024, OpenAI announced its "o3" model.[157] Partnering with ARC-AGI, it is claimed that the model effectively conquered the benchmark with a score of 87.5% using "high-compute" and 75.7% with lower compute.[158] For our purposes, o3 is directionally significant – it likely extends the qualitative trend in o1 of limited adaptation to novelty, but without resolution of fundamental shortcomings.

Public commentary[159] produced confusion about these results. Like o1, o3 was tested on the public ARC-AGI leaderboard. Public leaderboard scores are verified against a semi-private evaluation set to produce a final score.[160] This is the weaker version of ARC-AGI given that some exposure to the data on which the model is tested is assumed to have leaked into its training (thus potentially inflating its score). The claim that it "solved" ARC-AGI-1 is inaccurate absent testing on the private evaluation set.

The high score also excludes compute restrictions, limiting its significance to novelty-adaptation under uncertainty[161] – that it required this compute indicates the system cannot bootstrap its way into new solutions for problems without a helping hand, so to speak. Additionally, OpenAI explicitly trained o3 on the publicly available training dataset[162] – this is a standard practice in machine learning, though inconsistent with the open-ended generalization ARC-AGI is designed to test (doing so effectively undermines the goal of testing a model's ability to acquire new skills for new problems, as it has trained on sufficiently similar data).

Thus, o3 is directionally significant, but this does not point toward resolving fundamental shortcomings given its training, its excessive compute, and secrecy[163] over its architecture (making a fuller evaluation difficult).[164] External testing will likely indicate the directional significance in o1.

Nevertheless, o3's design may be moving in the neuro-symbolic direction (ARC founder François Chollet believes it already is neuro-symbolic[165]). Public spasms of euphoria and doom should not distract

Open AI CEO Sam Altman delivers a speech during the "Transforming Business through AI" event in Tokyo, Japan, on Feb. 3, 2025. (Tomohiro Ohsumi / Getty Images)

policymakers from understanding that much more work needs to be done – the capability measures that have marked AI's progress from AlexNet to o3 are not sufficient for enduring American leadership.

The U.S. Can Lead the Third Wave of AI

A Third Wave of AI development is needed: The strongest contender for this is neuro-symbolic AI. This approach seeks to build on the strengths of the first two waves while mitigating their shortcomings.

Scientific revolutions tend to exhibit a "conservativism"[166] in that they preserve the things worth preserving in earlier paradigms while simultaneously transforming the current understanding. The first two waves produced techniques worth preserving. Indeed, Artur d'Avila Garcez and Luís C. Lamb argue that neuro-symbolic AI should be the Third Wave in which symbolic and neural techniques are coupled to progress on foundational issues.[167]

Precedents exist for neuro-symbolic AI, though they are underplayed.

Researchers explicitly describe DeepMind's AlphaGeometry – a theorem-proving model – as neuro-symbolic, as it links a rule-based (symbolic)

David Ferris, global head of Cohere, Dan Tadross, head at Scale AI, and Jim Mitre, vice president and director of RAND Global, testify at the Senate Armed Services hearing on artificial intelligence cyber capabilities, on March 25, 2025, in Washington, DC. (Al Drago/Getty Images)

engine with a generative language model (neural).[168] AlphaGeometry 2 and AlphaProof[169] follow this hybrid[170] design. Gary Marcus[171] suggests that DeepMind's protein structure-predicting AlphaFold[172] – of recent Nobel[173] prestige – also possesses a (downplayed) neuro-symbolic structure.

Meta's[174] Cicero, built to play the strategy game (and longstanding AI challenge) Diplomacy,[175] is a beautifully hybrid system, a collection of specialized modules acting within a prespecified and hierarchical structure to handle planning, intent-formation, and communication with other players.[176] Echoing Deep Blue, input from expert human players was substantively integrated into the construction of the system – not a case of mere learning from the data and scaling up the model. Even AlphaGo, Henry Kautz argues, is a "prototypical" example of neuro-symbolic AI in its coupling of a problem-solver search algorithm with a neural network.[177] Despite the description of AlphaGo Zero as starting "tabula rasa"[178] by DeepMind researchers, Marcus correctly points out that the search algorithm was built-in rather than learned from the data.[179]

Finally, the ASU research group put forward a "generate-test" framework in which LLMs are inserted in a loop with a symbolic verifier, allowing the LLM to generate outputs and then improve their generation using the verifier's feedback as it checks their answers. This framework couples the expressiveness of LLMs and their ability to translate problems between formats (i.e., their relative open-endedness) with the domain-specific verifier to guarantee their accuracy (i.e., performance guarantees in critical domains). The generate-test framework improves LLMs' performance and is applicable to the o1 models.[180]

Existing U.S. Government Interest in Neuro-Symbolic AI

By choosing neuro-symbolic AI, policymakers are in good company. DARPA established its Assured Neuro Symbolic Reasoning (ANSR)[181] program in 2022, seeking to "integrate symbolic reasoning with data-driven learning to create robust, assured, and therefore trustworthy systems" and "repair defects in state-of-the-art " machine learning. This follows DARPA's 2018 announcement that it would $2 billion in Third Wave AI systems capable of adapting to new contexts.[182]

The NSF has expressed (comparatively limited) interest in funding neuro-symbolic research. A 2023 program solicitation for National AI Research Institutes detailing the needs of next-generation AI systems lays out three goals: grounding (understanding and robust engagement with concepts and an ability to reason over them), instructibility (effective human control), and alignment (operations consistent with objective, domain-specific truths and human intentions).[183] Neuro-symbolic AI is listed as one possible approach to accomplishing these goals. The reason bears on the lack of responsiveness of data-centric models to these goals without verifiable confidence in future breakthroughs through these techniques.[184] Deep neural networks and the generative models they have spawned cannot guarantee reliability and explainability.[185]

In July 2021, the NSF Division of Information and Intelligent Systems awarded University of South Carolina AI researcher Amit Sheth a $139,999 grant based on a proposal that explicitly invokes the first two waves of AI, arguing that neuro-symbolic AI is the foundation of the Third Wave.[186] The project focuses on the use of "knowledge graphs." Such graphs, as Desta Hagos and Danda Rawat note, represent the relationships between bits of information, thereby serving as a "structured network of interconnected concepts and entities."[187]

An interesting, if subtle, linkage exists between Sheth's NSF-funded work and the AI Research Institutes. In the special issue of "AI Magazine" in which Institute Program Director James Donlon explained their significance, an article coauthored by Sheth and Manas Gaur appears as an issue highlight. The subject: the coupling of generative language models with symbolic techniques (e.g., knowledge-infused ensembles of language models) for critical applications in health care.[188]

Echoes of the U.S. government's role in the foundations of the First Wave reverberate. The goal is to stake out suitable paths forward today without succumbing to earlier perils.

The following message thus drives the recommendations below: American AI leadership is increasingly defined by machine learning. Deference to the infrastructural needs of this technology (and others) has its benefits – including shoring up domestic semiconductor manufacturing capacity[189] and a 19% projected increase in the U.S.'s capture of private-sector investment in wafer fabrication from 2024-2032 thanks to the CHIPS Act[190] – but algorithmic- and architectural-level breakthroughs will be needed to expand American AI leadership; new ideas, not just new chips.

Recommendations for U.S. AI Leadership

Four recommendations reconceive U.S. AI leadership according to this understanding:

1. **The National Artificial Intelligence Initiative Office should direct the AI R&D Interagency Working Group to prioritize neuro-symbolic AI.**

   The federal AI R&D Interagency Working Group's mandate to promote long-term AI investments that conform with U.S. AI leadership should be leveraged to promote neuro-symbolic AI. The NAIIO, together with the Subcommittee on Machine Learning and AI, should therefore direct the IWG to prioritize investments in neuro-symbolic techniques.

   Such investments should be conceived as laying the foundations for U.S. leadership in the Third Wave, targeting deficiencies in AI systems like factual accuracy, reasoning, and planning, abstraction and generalization, and explainability. These investments should simultaneously be seen as pathways to models capable of robustly supporting applications.[191]

2. **The National Science Foundation should establish a national AI research institute for neuro-symbolic AI.**

   Per the National AI Research Institutes' development thus far,[192] a new institute should be established for neuro-symbolic research with an investment worth up to at least $20 million over five years. The purpose of this institute would be to complement existing work in the private sector by bringing together different research traditions while also expanding the reach of basic neuro-symbolic research for socially relevant applications.

   An institute for neuro-symbolic AI should engage in public-private collaboration in earnest, prioritizing

those actors willing to collaborate on innovative research in this emerging paradigm. Corporate partners like Meta and Google DeepMind, which are notable for their willingness to invest in neuro-symbolic research across strategic reasoning (Cicero and possibly AlphaGo), mathematics (AlphaGeometry and AlphaProof), and even biological research (AlphaFold), are leading contenders. Equally important are academic partners like Carnegie Mellon, the University of South Carolina, and others. Finally, since the AI Research Institutes emphasize collaboration with international researchers,[193] forming alliances with researchers and organizations within likeminded states is worthwhile.

Importantly, an institute for neuro-symbolic AI should avoid the pitfalls of Strategic Computing and the perils of over-ambitiousness in program and research design. Such an institute should decidedly not aim for AGI, conceived as the hypothetical endpoint of AI. Instead, basic research should be linked to applications in critical domains where current approaches fall short while ensuring its diffusion across the research ecosystem. Fortunately, the AI Research Institutes, pursue the U.S.'s AI objectives in part through complementarity with the private sector (taking high-risk, high-reward projects) and in part through use-inspired research that takes this link seriously.

The matter cannot be settled here, but critical applications in health care – including tasks related to mental health counseling, diagnostics, and clinical guidance, among others – are prime targets for neuro-symbolic research. These should be seriously considered in the establishment of an institute for neuro-symbolic AI.

3. **The U.S. Congress should fulfill the promise of the CHIPS Act by increasing federal agencies' basic research budgets.**

   The budget cuts for basic research funding at agencies including the NSF, NIH, and DoD – contra CHIPS Act expectations – should be reversed. These agencies must have the funds necessary to not only continue to reap the benefits of AI's Second Wave but also invest in foundational research of a sufficiently interdisciplinary nature for its Third Wave.

   There is historical precedent for the U.S. government over-indulging in AI R&D, with Strategic Computing being the archetypal example. The U.S. must take steps to avoid this fate again in a renewed era of great power competition without losing the vibrancy of its federal research ecosystem. The force of these recommendations is that bodies like the NAIIO and the NSF can secure American leadership in the Third Wave by complementing the progress made in the Second; acting as a source of "patient capital"[194] that firms up the foundations of American power[195] by wisely investing the resources it possesses today so that it has that same luxury tomorrow.

4. **The U.S. Congress and Commerce Department should adopt proactive yet targeted export controls on hardware and models in coordination with partners and allies.**

   The U.S. Congress and Commerce Department should ensure that its export controls on hardware or models are aggressively proactive yet targeted, proportional to the actual capabilities of the AI systems they enable or constitute, and implemented in coordination with partners and allies.

   Export controls are effectively a time-buying mechanism;[196] a necessary tool to blunt Chinese firms' efforts to develop AI models on the scale of their American counterparts. By leading the Third Wave, however, the U.S. can achieve two goals simultaneously: curb Chinese companies' advancements in machine learning – effectively restricting them to the Second Wave – while laying the foundations to reap the benefits of neuro-symbolic AI.

   It also, by implication, positions the U.S.'s frontier research to effectively surmount the longer-term diminishing returns of export controls as innovations beyond compute- and data-intensive machine learning unfold.

These recommendations should not be seen as exhaustive. Nor, furthermore, should U.S. policymakers expect the Third Wave to be free of hype cycles. When and if this time comes, it will be incumbent upon U.S. policymakers to be more vigilant in identifying persistent shortcomings in state-of-the-art

neuro-symbolic models and begin looking to the future. But the neuro-symbolic train has not yet left the station.

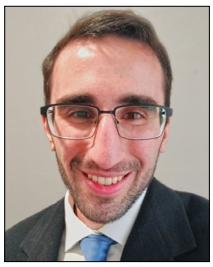
Conclusion

A classic gripe in the machine learning community today is that Marvin Minsky, that pivotal figure in early AI, was so disinterested in the use of ANNs, rather than his favored rule-based systems, that his near-ideological resistance set the field back decades. Imagine, the gripe goes, if neural nets were given their due in the 20 century – LLMs may have been decades old by now!

Putting aside the usual rebuttal to this – that the scaling up required to bring neural networks to their current glory depended on access to hardware that did not exist in Minsky's heyday – the message is clear: Over-indulgence in fundamentally limited symbolic AI harmed the field.

Today, the field risks nurturing a generation of Minskys. This time, machine learning is favored above all else. Their original message, however, remains true: over-indulgence in a fundamentally limited paradigm harms the field. AI is now in the spotlight, a critical technology[197] that promises to be the crown jewel of American technological leadership – such indulgences can no longer be afforded.

America has the resources and the will to lead in AI. It should not squander its opportunity by mistaking machine learning for this technology's endgame.



Vincent J. Carchidi is an analyst focusing on critical and emerging technologies in U.S.-China technology competition and the Middle East. He is a Non-Resident Scholar at the Middle East Institute's Strategic Technologies and Cyber Security Program. He is also a Non-Resident Fellow at the Orion Policy Institute specializing in AI policy. His tech policy work appears in outlets including Defense One, National Interest, The Hill, Trends Research & Advisory, and the Foreign Policy Research Institute. Carchidi maintains a background in cognitive science, applying this research to the trajectories and limitations of frontier AI models. His opinions are his own. You can follow him on LinkedIn, BlueSky, and X.

Endnotes

1 Garcez, A.d. & Lamb, L.C. (2023). Neurosymbolic AI: the 3rd wave. Artificial Intelligence Review, 56(11), 12387-12406. https://doi.org/10.1007/s10462-023-10448-w.

2 Iyengar, R. (2024, August 16). The technocrat. Foreign Policy. https://foreignpolicy.com/2024/08/16/gina-raimondo-us-china-tech-competition-chips-ai/.

3 Hawkins, M. (2024, October 9). U.S. debates who should be able to buy American AI chips. Bloomberg. https://www.bloomberg.com/news/newsletters/2024-10-09/us-debates-whether-to-let-american-chips-fuel-growth-of-global-ai.

4 Hammond, S. (2024). The scramble for AI computing power. American Affairs, VIII(2). https://americanaffairsjournal.org/2024/05/the-scramble-for-ai-computing-power/.

5 Deese, B. and Hansmann, L. (2024, September 12). America needs an energy policy for AI. Heatmap. https://heatmap.news/technology/ai-additionality-framework.

6 Dean, J. (2019). The Deep Learning Revolution and its implications for computer architecture and chip design. ArXiv, 1-17. https://doi.org/10.48550/arXiv.1911.05289.

7 For an accessible overview of the increase in computational demands through the deep learning revolution and how this relates to capabilities, see, Christopher Summerfield. (2023). Natural general intelligence: How understanding the brain can help us build AI. Oxford University Press, 51-60.

8 U.S.-China Economic and Security Review Commission. (2024). 2024 Report to Congress of the U.S.-China Economic and Security Review Commission. U.S. Government Publishing Office. https://www.uscc.gov/sites/default/files/2024-11/2024_Annual_Report_to_Congress.pdf: 27.

9 Zegart, A. (2024, August 20). The crumbling foundations of American strength. Foreign Affairs. https://www.foreignaffairs.com/united-states/crumbling-foundations-american-strength-amy-zegart.

10 Bajraktari, Y. (2024, September 30). The Artificial General Intelligence presidency is coming. Foreign Policy. https://foreignpolicy.com/2024/09/30/artificial-general-intelligence-agi-president/

11 Defense Advanced Research Projects Agency. (1983). Strategic computing: New-Generation computing technology: A strategic plan for its development and application to critical problems in defense (NTIS Issue No.198419). National Technical Reports Library, U.S. Department of Commerce. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA141982.xhtml.

12 See, Nilsson, N.J. (2009). The Quest for artificial intelligence. Cambridge University Press, ch. 23; Salisbury, E. (2020, May 22). A cautionary tale on ambitious feats of AI: The Strategic computing program. War on the Rocks. https://warontherocks.com/2020/05/cautionary-tale-on-ambitious-feats-of-ai-the-strategic-computing-program/.

13 On this cycle, see, Richbourg, R. (2018, May 10). 'It's either a Panda or a Gibbon': AI Winters and the limits of deep learning. War on the Rocks. https://warontherocks.com/2018/05/its-either-a-panda-or-a-gibbon-ai-winters-and-the-limits-of-deep-learning/.

14 Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J.C., Shoham, Y., Wald, R., & Clark, J. (2024). Artificial Intelligence index report 2024. Stanford University Human-Centered Artificial Intelligence. https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf, 244.

15 Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J.C., Shoham, Y., Wald, R., & Clark, J. (2024). Artificial Intelligence index report 2024. Stanford University Human-Centered Artificial Intelligence. https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf, 247.

16 Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J.C., Shoham, Y., Wald, R., & Clark, J. (2024). Artificial Intelligence index report 2024. Stanford University Human-Centered Artificial Intelligence. https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf, 403.

17 Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J.C., Shoham, Y., Wald, R., & Clark, J. (2024). Artificial Intelligence index report 2024. Stanford University Human-Centered Artificial Intelligence. https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf, 403.

18 Launchbury, J. (2017). A DARPA perspective on artificial intelligence [PowerPoint slides]. https://web.archive.org/web/20161215001731/https://www.darpa.mil/attachments/AIFull.pdf.

19 Defense Advanced Research Projects Agency. (2018). AI next campaign. https://web.archive.org/web/20180908120032/https://www.darpa.mil/work-with-us/ai-next-campaign.

20 National Research Council. (1999). Funding a revolution: Government support for computing research. National Academies Press, 198-205.

21 National Research Council. (1999). Funding a revolution: Government support for computing research. National Academies Press, 199-201.

22 McCarthy, J., Minsky, M.L., Rochester, N., & Shannon, C.E. (1955/2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. AI Magazine, 27(4), 12-14. https://doi.org/10.1609/aimag.v27i4.1904.

23 National Research Council. (1999). Funding a revolution: Government support for computing research. National Academies Press, 202-203.

24 National Research Council. (1999). Funding a revolution: Government support for computing research. National Academies Press, 204.

25 National Research Council. (1999). Funding a revolution: Government support for computing research. National Academies Press, 205.

26 Nilsson, N.J. (2009). The Quest for Artificial Intelligence. Cambridge University Press, 286; see also, National Research Council. (1999). Funding a revolution: Government support for computing research. National Academies Press, 212-213.

27 Symbolic AI is sometimes referred to as "good old-fashioned AI." See, Togelius, J. (2024). Artificial general intelligence. The MIT Press, 84.

28 See, Hagos, D. H. & Rawat, D. B. (2024). Neuro-Symbolic AI for military applications. ArXiv, 2. https://arxiv.org/abs/2408.09224v2; in contrast to the "black box" nature of a deep neural network, a Symbolic system is sometimes called a "white-box system." Feldstein, J., Dilkas, P., Belle, V., & Tsamoura, E. (2024). Mapping the Neuro-Symbolic AI landscape by architectures: A handbook on augmenting deep learning through symbolic reasoning. ArXiv, 3. https://doi.org/10.48550/arXiv.2410.22077.

29 Strickland, E. (2021, September 30). The turbulent past and uncertain future of artificial intelligence. IEEE Spectrum. https://spectrum.ieee.org/history-of-ai.

30 Nilsson, N.J. (2009). The quest for artificial intelligence. Cambridge University Press, 286-287.

31 Feigenbaum, E.A. & McCorduck, P. (1983). The Fifth Generation: Artificial Intelligence and Japan's Computer Challenge to the World. Addison-Wesley.

32 Garvey, C. (2019). Artificial Intelligence and Japan's Fifth Generation: The Information Society, Neoliberalism, and Alternative Modernities. Pacific Historical Review, 88(4), 646. https://doi.org/10.1525/phr.2019.88.4.619.

33 Nilsson, N.J. (2009). The quest for artificial intelligence. Cambridge University Press, 288.

34 National Research Council. (1999). Funding a revolution: Government support for computing research. National Academies Press, 206-207.

35 National Research Council. (1999). Funding a revolution: Government support for computing research. National Academies Press, 207.

36 Salisbury, E. (2020, May 22). A cautionary tale on ambitious feats of AI: The Strategic Computing program. War on the Rocks. https://warontherocks.com/2020/05/cautionary-tale-on-ambitious-feats-of-ai-the-strategic-computing-program/.

37 Salisbury, E. (2020, May 22). A cautionary tale on ambitious feats of AI: The Strategic Computing program. War on the Rocks. https://warontherocks.com/2020/05/cautionary-tale-on-ambitious-feats-of-ai-the-strategic-computing-program/.

38 Rosenblatt, F. (1957). The Perceptron: A perceiving and recognizing automation (Project PARA). Cornell Aeronautical Laboratory, Inc. https://bpb-us-e2.wpmucdn.com/websites.umass.edu/dist/a/27637/files/2016/03/rosenblatt-1957.pdf.

39 See, Haigh, T. (2024, October 8). Between the booms: AI in Winter. Communications of the ACM. https://cacm.acm.org/opinion/between-the-booms-ai-in-winter/#B4.

40 Irwin, J. A. (2024). Artificial worlds and perceptronic objects: The CIA's mid-century automatic target recognition. Grey Room, 97, 17-20. https://doi.org/10.1162/grey_a_00415.

41 The Nobel Prize Organisation. (2024, October 8). The Nobel Prize in Physics 2024. https://www.nobelprize.org/prizes/physics/2024/press-release/

42 National Science Foundation. (2024, October 8). NSF congratulates laureates of the 2024 Nobel Prize in physics. https://new.nsf.gov/news/nsf-congratulates-laureates-2024-nobel-prize-physics.

43 Horowitz, M.C., Allen, G.C., Kania, E.B., & Scharre, P. (2018). Strategic competition in an era of artificial intelligence. Center for a New American Security. https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS-Strategic-Competition-in-an-Era-of-AI-July-2018_v2.pdf, 6.

44 Badlam, J., Clark, S., Gajendragadkar, S., Kumar, A., O'Rourke, S., & Swartz, D. (2024, May 16). The CHIPS and Science Act: here's what's in it. McKinsey & Company. https://www.mckinsey.com/industries/public-sector/our-insights/the-chips-and-science-act-heres-whats-in-it.

45 Zegart, A. (2024, August 20). The crumbling foundations of American strength. Foreign Affairs. https://www.foreignaffairs.com/united-states/crumbling-foundations-american-strength-amy-zegart.

46 See, National Science Foundation. National Artificial Intelligence Research Institutes. https://new.nsf.gov/funding/opportunities/national-artificial-intelligence-research-institutes

47 Donlon, J.J. (2024). The National Artificial Intelligence Research Institutes program and its significance to a prosperous future. AI Magazine, 45(1), 6. https://doi.org/10.1002/aaai.12153.

48 Donlon, J.J. (2024). The National Artificial Intelligence Research Institutes program and its significance to a prosperous future. AI Magazine, 45(1), 6. https://doi.org/10.1002/aaai.12153.

49 Donlon, J.J. (2024). The National Artificial Intelligence Research Institutes program and its significance to a prosperous future. AI Magazine, 45(1), 6-8. https://doi.org/10.1002/aaai.12153; see also, Select Committee on Artificial Intelligence of the National Science and Technology Council. (2023). National artificial intelligence research and development strategic plan 2023 update. Executive Office of the President of the United States. https://www.nitrd.gov/pubs/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf.

50 Donlon, J.J. (2024). The National Artificial Intelligence Research Institutes program and its significance to a prosperous future. AI Magazine, 45(1), 10. https://doi.org/10.1002/aaai.12153.

51 Donlon, J.J. (2024). The National Artificial Intelligence Research Institutes program and its significance to a prosperous future. AI Magazine, 45(1), 11. https://doi.org/10.1002/aaai.12153.

52 See, Kalil. T. (2016, May 6). Charter of the Subcommittee on Machine Learning and Artificial Intelligence, Committee on Technology, National Science and Technology Council. Executive Office of the President of the United States. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/NSTC/ai_charter_-_signed_final.pdf.

53 See, Networking and Information Technology Research and Development. Artificial Intelligence R&D Interagency Working Group. https://www.nitrd.gov/coordination-areas/ai/.

54 Subcommittee on the Networking & Information Technology Research & Development and the Subcommittee on Machine Learning & Artificial Intelligence of the National Science & Technology Council. (2024). The Networking & Information Technology R&D Program and the National Artificial Intelligence Initiative Office Supplement to the President's FY2025 Budget. Executive Office of the President of the United States, National Science and Technology Council. https://www.nitrd.gov/pubs/FY2025-NITRD-NAIIO-Supplement.pdf: 20.

55 Subcommittee on Networking & Information Technology Research & Development, Machine Learning & Artificial Intelligence Subcommittee, & National Science & Technology Council. (2023). The Networking & Information Technology R&D Program and the National Artificial Intelligence Initiative Office supplement to the president's FY 2024 budget. Executive Office of the President of the United States. https://www.nitrd.gov/pubs/FY2024-NITRD-NAIIO-Supplement.pdf: 27-28.

56 H.R. 6395 – 1136. National Artificial Intelligence Initiative Act of 2020. https://www.aip.org/sites/default/files/aipcorp/images/fyi/pdf/national-ai-initiative-act-final.pdf: Sec. 5201.

57 Subcommittee on Networking & Information Technology Research & Development, Machine Learning & Artificial Intelligence Subcommittee, & National Science & Technology Council. (2023). The Networking & Information Technology R&D Program and the National Artificial Intelligence Initiative Office supplement to the president's FY 2024 budget. Executive Office of the President of the United States. https://www.nitrd.gov/pubs/FY2024-NITRD-NAIIO-Supplement.pdf, 83.

58 Subcommittee on Networking & Information Technology Research & Development, Machine Learning & Artificial Intelligence Subcommittee, & National Science & Technology Council. (2023). The Networking & Information Technology R&D Program and the National Artificial Intelligence Initiative Office supplement to the president's FY 2024 budget. Executive Office of the President of the United States. https://www.nitrd.gov/pubs/FY2024-NITRD-NAIIO-Supplement.pdf, 83.

59 Ornstein, S. M., Smith, B. C., & Suchman, L. A. (1984). Strategic computing. Bulletin of the Atomic Scientists, 40(10), 12. https://doi.org/10.1080/00963402.1984.11459292.

60 Krizhevsky, A., Sutskever, I., & Hinton, G.E. (2012). ImageNet classification with deep Convolutional Neural Networks. NeurIPS Proceedings, 1-9. https://papers.nips.cc/paper_files/paper/2012/file/c399862d3b9d6b76c8436e924a68c45b-Paper.pdf

61 Dean, J. (2019). The Deep Learning Revolution and its implications for computer architecture and chip design. ArXiv, 1-3. https://doi.org/10.48550/arXiv.1911.05289.

62 Denton, E., Hanna, A., Amironesei, R., Smart, A., & Nicole, H. (2021). On the genealogy of machine learning datasets: A critical history of ImageNet. Big Data & Society, 8(2), 5-6. https://journals.sagepub.com/doi/epdf/10.1177/20539517211035955.

63 Sample, I. (2023, October 28). Race to AI: The origins of artificial intelligence, from Turing to ChatGPT. The Guardian. https://www.theguardian.com/technology/2023/oct/28/artificial-intelligence-origins-turing-to-chatgpt

64 The Economist. (2024, June 30). The race is on to control the global supply chain for AI chips. The Economist. https://www.economist.com/schools-brief/2024/07/30/the-race-is-on-to-control-the-global-supply-chain-for-ai-chips.

65 Moyer, C. (2016, March 28). How Google's AlphaGo beat a Go world champion. The Atlantic. https://www.theatlantic.com/technology/archive/2016/03/the-invisible-opponent/475611/.

66 See generally, Silver, D. et al. (2016). Mastering the game of Go with deep neural networks and tree search. Nature, 529(7587), 484–489. https://doi.org/10.1038/nature16961.

67 Silver, D. et al. (2016). Mastering the game of Go with deep neural networks and tree search. Nature, 529(7587), 491. https://doi.org/10.1038/nature16961.

68 Silver, D. et al. (2016). Mastering the game of Go with deep neural networks and tree search. Nature, 529(7587), 487. https://doi.org/10.1038/nature16961.

69 Silver, D. & Hassabis, D. (2017, October 18). AlphaGo Zero: Starting from scratch. Google DeepMind. https://deepmind.google/discover/blog/alphago-zero-starting-from-scratch/.

70 See generally, Silver, D. et al. (2017). Mastering the game of Go without human knowledge. Nature, 550(7676), 354–359. https://doi.org/10.1038/nature24270.

71 Silver, D. et al. (2017). Mastering the game of Go without human knowledge. Nature, 550(7676), 361. https://doi.org/10.1038/nature24270.

72 Goodrich, J. (2021, January 25). How IBM's Deep Blue beat world champion Chess player Garry Kasparov. IEEE Spectrum. https://spectrum.ieee.org/how-ibms-deep-blue-beat-world-champion-chess-player-garry-kasparov.

73 Thompson, C. (2022, February 18). What the history of AI tells us about its future. MIT Technology Review. https://www.technologyreview.com/2022/02/18/1044709/ibm-deep-blue-ai-history/.

74 Silver, D. et al. (2016). Mastering the game of Go with deep neural networks and tree search. Nature, 529(7587), 489. https://doi.org/10.1038/nature16961.

75 Turing, A. M. (1950). Computing machinery and intelligence. Mind, LIX(236), 433–460. https://doi.org/10.1093/mind/LIX.236.433.

76 Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, L., & Polosukhin, I. (2017). Attention is all you need. ArXiv, 1–15. https://doi.org/10.48550/arXiv.1706.03762

77 Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). Language models are unsupervised multitask learners. OpenAI, 1–24. https://cdn.openai.com/better-language-models/language_models_are_unsupervised_multitask_learners.pdf.

78 Brown, T.B. et al. (2020). Language models are few-shot learners. ArXiv, 1–75. https://doi.org/10.48550/arXiv.2005.14165.

79 This is the overview provided by Summerfield, who notes that the test suffers from being ill-defined and deficient. Yet, GPTs are effectively novel memory algorithms whose information selection is more contextually relevant than past NLP systems. See, Christopher Summerfield. (2023). Natural general intelligence: How understanding the brain can help us build AI. Oxford University Press, 20–24.

80 Brown, T.B. et al. (2020). Language models are few-shot learners. ArXiv, 8–9. https://doi.org/10.48550/arXiv.2005.14165.

81 Garisto, D. (2024, June 4). How cutting-edge computer chips are speeding up the AI revolution. Nature. https://www.nature.com/articles/d41586-024-01544-0.

82 OpenAI. (2022, November 30). Introducing ChatGPT. OpenAI. https://openai.com/index/chatgpt/.

83 OpenAI. (2023, March 13). GPT-4 is OpenAI's most advanced system, producing safer and more useful responses. OpenAI. https://openai.com/index/gpt-4/

84 OpenAI et al. (2023). GPT-4 technical report. ArXiv, 2. https://doi.org/10.48550/arXiv.2303.08774.

85 The Epoch AI Team. (2023, October 23). Announcing Epoch AI's updated parameters, compute, and data trends database. Epoch AI. https://epochai.org/blog/announcing-updated-pcd-database

86 Subin, S. (2025, February 8). Tech megacaps plan to spend more than $300 billion in 2025 as AI race intensifies. CNBC. https://www.cnbc.com/2025/02/08/tech-megacaps-to-spend-more-than-300-billion-in-2025-to-win-in-ai.html.

87 Siripurapu, A. & Berman, N. (2024, May 14). The contentious U.S.-China trade relationship. Council on Foreign Relations. https://www.cfr.org/backgrounder/contentious-us-china-trade-relationship.

88 Alper, A., Sterling, T. & Nellis, S. (2020, January 6). Trump administration pressed Dutch hard to cancel China chip-equipment sale – sources. Reuters. https://www.reuters.com/article/world/uk/trump-administration-pressed-dutch-hard-to-cancel-china-chip-equipment-sale-so-idUSKBN1Z50H4/

89 Clark, D. (2021, July 4). The tech Cold War's 'Most Complicated Machine' that's out of China's reach. The New York Times. https://www.nytimes.com/2021/07/04/technology/tech-cold-war-chips.html

90 The Eurasia Group. (2020). The geopolitics of semiconductors. Eurasia Group. https://www.eurasiagroup.net/files/upload/Geopolitics-Semiconductors.pdf, 8.

91 Shepardson, D., Freifeld, K., & Alper, A. (2020, May 15). U.S. moves to cut Huawei off from global chip suppliers as China eyes retaliation. Reuters. https://www.reuters.com/article/technology/us-moves-to-cut-huawei-off-from-global-chip-suppliers-as-china-eyes-retaliatio-idUSKBN22R1IP/.

92 Soliman, M. & Carchidi, V. (2024, May 16). Technology policy: Convergence and crossroads in Biden vs. Trump 2.0. Foreign Policy Research Institute. https://www.fpri.org/article/2024/05/technology-policy-biden-vs-trump/.

93 Nellis, S. & Lee, J. (2022, September 1). U.S. officials order Nvidia to halt sales of top AI chips to China. Reuters. https://www.reuters.com/technology/nvidia-says-us-has-imposed-new-license-requirement-future-exports-china-2022-08-31/.

94 Bureau of Industry and Security. (2022, October 7). Commerce implements new export controls on advanced computing and semiconductor manufacturing items to the People's Republic of China (PRC) [Press release]. https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file.

95 Sevastopulo, D. & Hille, K. (2022, October 7). U.S. hits China with seeping tech export controls. Financial Times. https://www.ft.com/content/6825bee4-52a7-4c86-b1aa-31c100708c3e.

96 Hammond, S. (2024). The scramble for AI computing power. American Affairs, VIII(2). https://americanaffairsjournal.org/2024/05/the-scramble-for-ai-computing-power/.

97 Hart, C. & Pitcher, J. (2024, September 17). BlackRock, Microsoft partner on massive new AI infrastructure fund. The Wall Street Journal. https://www.wsj.com/tech/ai/blackrock-global-infrastructure-partners-microsoft-mgx-launch-ai-partnership-1d00e09f.

98 Microsoft Source. (2024, September 17). BlackRock, Global Infrastructure Partners, Microsoft and MGX launch new AI partnership to invest in data centers and supporting power infrastructure. Microsoft. https://news.microsoft.com/2024/09/17/blackrock-global-infrastructure-partners-microsoft-and-mgx-launch-new-ai-partnership-to-invest-in-data-centers-and-supporting-power-infrastructure/.

99 Masters, B., Gara, A., Fontanella-Khan, J., & Morris, S. (2024, September 17). BlackRock and Microsoft plan $30bn fund to invest in AI infrastructure. Financial Times. https://www.ft.com/content/44411l4b-a105-439c-949b-1e7f8151 7deb.

100 Zeitlin, M. (2024, September 20). Microsoft's mega deal is a massive victory for nuclear power. Heatmap. https://heatmap.news/economy/microsoft-three-mile-island-nuclear-constellation; Terrell, M. (2024, October,14). New nuclear clean energy agreement with Kairos Power. Google. https://blog.google/outreach-initiatives/sustainability/google-kairos-power-nuclear-energy-agreement/.

101 Bureau of Industry and Security. (2025, January 13). Biden-Harris administration announces regulatory framework for the Responsible Diffusion of Advanced Artificial Intelligence Technology [Press release]. https://www.bis.gov/press-release/biden-harris-administration-announces-regulatory-framework-responsible-diffusion.

102 Soliman, M. (2025, January 16). Digital borders: The Biden administration's final AI rule. The National Interest. https://nationalinterest.org/blog/techland/digital-borders-biden-administrations-final-ai-rule-214416.

103 Leonard, J. & Koc, C. (2023, January 27). Biden nears win as Japan, Dutch back China chip controls. Bloomberg. https://www.bloomberg.com/news/articles/2023-01-27/japan-netherlands-to-join-us-in-chip-export-controls-on-china.

104 Koc, C. & Leonard, J. (2024, August 29). ASML's China chip business faces new curbs from Netherlands. Bloomberg. https://www.bloomberg.com/news/articles/2024-08-29/the-netherlands-to-put-more-curbs-on-asml-s-china-chip-business

105 Hawkins, M., King, I., Koc, C., & Mochizuki, T. (2024, July 17). U.S. floats idea of tougher trade rules in chip crackdown on China. Bloomberg. https://www.bloomberg.com/news/articles/2024-07-17/us-considers-tougher-trade-rules-against-companies-in-chip-crackdown-on-china.

106 Sterling, T. (2024, September 6). Dutch government retakes export control over two ASML tools from US. Reuters. https://www.reuters.com/technology/dutch-government-retakes-export-control-over-two-asml-tools-us-2024-09-06/.

107 For a more detailed history of US-led export controls and their global interactions, see, Carchidi, V. & Soliman, M. (2024). The role of the Middle East in the US-China race to AI supremacy. Middle East Institute. https://www.mei.edu/publications/role-middle-east-us-china-race-ai-supremacy: 11-27.

108 Hagey, K. & Fitch, A. (2024, February 8). Sam Altman seeks trillions of dollars to reshape business of chips and AI. The Wall Street Journal. https://www.wsj.com/tech/ai/sam-altman-seeks-trillions-of-dollars-to-reshape-business-of-chips-and-ai-89ab3db0.

109 Ghaffary, S. & Ludlow, E. (2024, April 10). OpenAI's Altman pitches global AI coalition on trip to Middle East. Bloomberg. https://www.bloomberg.com/news/articles/2024-04-10/openai-s-altman-pitches-global-ai-coalition-on-trip-to-middle-east

110 Ghaffary, S. & Hawkins, M. (2024, September 3). Altman infrastructure plan aims to spend tens of billions in US. Bloomberg. https://www.bloomberg.com/news/articles/2024-09-03/altman-infrastructure-plan-aims-to-spend-tens-of-billions-in-us

111 Hu, K., Potkin, F., & Nellis, S. (2024, October 30). Exclusive: OpenAI builds first chip with Broadcom and TSMC, scales back foundry ambition. Reuters. https://www.reuters.com/technology/artificial-intelligence/openai-builds-first-chip-with-broadcom-tsmc-scales-back-foundry-ambition-2024-10-29/.

112 Cornish, C. & Murgia, M. (2024, March 15). Abu Dhabi in talks to invest in OpenAI chip venture. Financial Times. https://www.ft.com/content/d018067f-20e7-49eb-83dc-ebb8b1aad1a5.

113 Metz, C. & Mickle, T. (2024, September 25). Behind OpenAI's audacious plan to make A.I. flow like electricity. The New York Times. https://www.nytimes.com/2024/09/25/business/openai-plan-electricity.html.

114 Hayden Field. (2024, November 13). OpenAI to present plans for U.S. AI strategy and an alliance to compete with China. CNBC. https://www.cnbc.com/2024/11/13/openai-to-present-plans-for-us-ai-strategy-and-an-alliance-to-compete-with-china.html; see also, Center for Strategic and International Studies. (2024, November 13). Ensuring U.S. leadership in AI: Industry perspective on data center growth. Center for Strategic and International Studies. https://www.csis.org/analysis/ensuring-us-leadership-ai-industry-perspective-data-center-growth.

115 Goldman, S. (2025, January 22). OpenAI's Stargate may be tech's biggest gamble ever, but here's what's really at stake. Fortune. https://fortune.com/2025/01/22/openai-stargate-ai-sam-altman-donald-trump/.

116 Altman, S. (2024, September 23). The intelligence age. Sam Altman. https://ia.samaltman.com/.

117 See, Kambhampati, S. (2023, September 12). Can LLMs really reason and plan? Communications of the ACM. https://cacm.acm.org/blogcacm/can-llms-really-reason-and-plan/.

118 Valmeekam, K., Olmo, A., Sreedharan, S., & Kambhampati, S. (2022). Large Language Models still can't plan (A benchmark for LLMs on planning and reasoning about change). ArXiv, 2. https://arxiv.org/abs/2206.10498v1.

119 Valmeekam, K., Marquez, M., Sreedharan, S., & Kambhampati, S. (2023). On the planning abilities of Large Language Models: A critical investigation. ArXiv, 5. https://arxiv.org/abs/2305.15771v2.

120 Valmeekam, K., Marquez, M., Sreedharan, S., & Kambhampati, S. (2023). On the planning abilities of Large Language Models: A critical investigation. ArXiv, 2. https://arxiv.org/abs/2305.15771v2.

121 See generally, Kambhampati, S. (2024). Can Large Language Models reason and plan? ArXiv, 1-5. https://doi.org/10.48550/arXiv.2403.04121.

122 Lewis, M. & Mitchell, M. (2024). Evaluating the robustness of analogical reasoning in Large Language Models. ArXiv, 1-31. https://doi.org/10.48550/arXiv.2411.14215. The authors re-test earlier work in addition to their own experiments. For the original work, see, Webb, T., Holyoak, K. J., & Lu, H. (2023). Emergent analogical reasoning in large language models. Nature, 7(9), 1526-1541. https://doi.org/10.1038/s41562-023-01659-w.

123 Lewis, M. & Mitchell, M. (2024). Evaluating the robustness of analogical reasoning in Large Language Models. ArXiv, 22. https://doi.org/10.48550/arXiv.2411.14215.

124 Lewis, M. & Mitchell, M. (2024). Evaluating the robustness of analogical reasoning in Large Language Models. ArXiv, 22. https://doi.org/10.48550/arXiv.2411.14215.

125 Xu, Z., Jain, S., & Kankanhalli, M. (2024). Hallucination is inevitable: An innate limitation of Large Language Models. ArXiv, 1-26. https://doi.org/10.48550/arXiv.2401.11817.

126 Banerjee, S., Agarwal, A., & Singla, S. (2024). LLMs will always hallucinate, and we need to live with this. ArXiv, 1-31. https://doi.org/10.48550/arXiv.2409.05746.

127 See, Gaur, M. & Sheth, A. (2024). Building trustworthy NeuroSymbolic AI systems: Consistency, reliability, explainability, and safety. AI Magazine, 45(1), 142-143. https://doi.org/10.1002/aaai.12149.

128 Udandarao, V., Prabhu, A., Ghost, A., Sharma, Y., Torr, P.H.S., Bibi, A., Albanie, S., & Bethge, M. (2024). No "Zero-Shot" without exponential data: Pretraining concept frequency determines multimodal model performance. ArXiv, 1-41. https://doi.org/10.48550/arXiv.2404.04125.

129 Mitchell, M., Palmarini, A.B., & Moskvichev, A. (2023). Comparing humans, GPT-4, and GPT-4V on abstraction and reasoning tasks. ArXiv, 1-12. https://doi.org/10.48550/arXiv.2311.09247.

130 Jiang, Y., Zhang, J., Sun, K., Sourati, Z., Ahrabian, K., Ma, K., Ilievski, F., & Pujara, J. (2024). MARVEL: Multidimensional abstraction and reasoning through visual evaluation and learning. ArXiv, 1-21. https://doi.org/10.48550/arXiv.2404.13591.

131 McCoy, R.T., Yao, S., Friedman, D., & Griffiths, T.L. (2024). Embers of autoregression show how large language models are shaped by the problem they are trained to solve. PNAS, 121(41), 2. https://doi.org/10.1073/pnas.2322420121.

132 Knoop, M. & Chollet, F. (2024). ARC prize. ARC Prize. https://arcprize.org/

133 Lab42. (2024). ARC: Abstraction & reasoning corpus. Lab42. https://lab42.global/arc/.

134 ARC Prize. (2024). ARC-AGI 2024 high scores. https://arcprize.org/leaderboard.

135 See generally, Goertzel, B. & Pennachin, C. (Eds). (2007). Artificial general intelligence. Springer.

136 Voss, P. & Jovanovic, M. (2024). Why we don't have AGI yet. ArXiv, 1. https://arxiv.org/abs/2308.03598v4.

137 OpenAI. (2024, September 12). Introducing OpenAI o1. https://openai.com/o1/

138 Robison, K. (2024, September 12). OpenAI releases o1, its first model with 'reasoning' abilities. The Verge. https://www.theverge.com/2024/9/12/24242439/openai-o1-model-reasoning-strawberry-chatgpt.

139 OpenAI. (2024, September 12). Introducing OpenAI o1-preview. https://openai.com/index/introducing-openai-o1-preview/

140 OpenAI. (2024). OpenAI o1 System Card. OpenAI, 1-43. https://assets.ctfassets.net/kftzwdyauwt9/67qJD51Aur3eIc96iOfeOP/71551c3d223cd97e591aa89567306912/o1_system_card.pdf.

141 Wei, J., Wang, X., Schuurmans, D., Bosma, M., Ichter, B., Xia, F., Chi, E., Le, Q., & Zhou, D. (2023). Chain-of-Thought prompting elicits reasoning in Large Language Models. ArXiv, 2. https://arxiv.org/abs/2201.11903v6.

142 On this possible architecture, see, Valmeekam, K., Stechly, K., Gundawar, A., & Kambhampati, S. (2024). Planning in strawberry fields: Evaluating and improving the planning and scheduling capabilities of LRM o1. ArXiv, 5, 13-14. https://doi.org/10.48550/arXiv.2410.02162.

143 Kahn, J. (2024, September 13). 9 things you need to know about OpenAI's powerful new AI model o1. Fortune. https://fortune.com/2024/09/13/openai-o1-strawberry-model-9-things-you-need-know/

144 ARC Prize. (2024). ARC-AGI-PUB 2024 high scores. https://arcprize.org/leaderboard#arc-agi-pub.

145 Knoop, M. (2024, September 13). OpenAI o1 results on ARC-AGI-PUB. ARC Prize. https://arcprize.org/blog/openai-o1-results-arc-prize.

146 Mirzadeh, I., Alizadeh, K., Shahrokhi, H., Tuzel, O., Bengio, S., & Farajtabar, M. (2024). GSM-Symbolic: Understanding the limitations of mathematical reasoning in Large Language Models. ArXiv, 1-5. https://doi.org/10.48550/arXiv.2410.05229.

147 Mirzadeh, I., Alizadeh, K., Shahrokhi, H., Tuzel, O., Bengio, S., & Farajtabar, M. (2024). GSM-Symbolic: Understanding the limitations of mathematical reasoning in Large Language Models. ArXiv, 8-9. https://doi.org/10.48550/arXiv.2410.05229.

148 Mirzadeh, I., Alizadeh, K., Shahrokhi, H., Tuzel, O., Bengio, S., & Farajtabar, M. (2024). GSM-Symbolic: Understanding the limitations of mathematical reasoning in Large Language Models. ArXiv, 10. https://doi.org/10.48550/arXiv.2410.05229.

149 Mirzadeh, I., Alizadeh, K., Shahrokhi, H., Tuzel, O., Bengio, S., & Farajtabar, M. (2024). GSM-Symbolic: Understanding the limitations of mathematical reasoning in Large Language Models. ArXiv, 19. https://doi.org/10.48550/arXiv.2410.05229.

150 McCoy, T.R., Yao, S., Friedman, D., Hardy, MD., & Griffiths, T.L. (2024). When a language model is optimized for reasoning, does it still show embers of autoregression? An analysis of OpenAI o1. ArXiv, 1. https://doi.org/10.48550/arXiv.2410.01792.

151 Lehman, J., Meyerson, E., El-Gaaly, T., Stanley, K.O., & Ziyaee, T. (2025). Evolution and the Knightian blindspot of machine learning. ArXiv, 22. https://doi.org/10.48550/arXiv.2501.13075.

152 Valmeekam, K., Stechly, K., Kambhampati, S. (2024). LLMs still can't plan; can LRMs? A preliminary evaluation of OpenAI's o1 on PlanBench. ArXiv, 1-3. https://doi.org/10.48550/arXiv.2409.13373.

153 See, Helmert, M. (2011). The Fast Downward planning system. ArXiv, 1-56. https://doi.org/10.48550/arXiv.1109.6051.

154 Valmeekam, K., Stechly, K., Kambhampati, S. (2024). LLMs still can't plan; can LRMs? A preliminary evaluation of OpenAI's o1 on PlanBench. ArXiv, 6. https://doi.org/10.48550/arXiv.2409.13373

155 Monroe, D. (2022, October 1). Neurosymbolic AI. Communications of the ACM. https://cacm.acm.org/news/neurosymbolic-ai/.

156 Marcus, G. (2018). Deep learning: A critical appraisal. ArXiv, 14. https://doi.org/10.48550/arXiv.1801.00631

157 Edwards, B. (2024, December 20). OpenAI announces o3 and o3-mini, its next simulated reasoning models. https://arstechnica.com/information-technology/2024/12/openai-announces-o3-and-o3-mini-its-next-simulated-reasoning-models/.

158 Chollet, F. (2024, December 20). OpenAI o3 breakthrough high score on ARC-AGI-PUB. https://arcprize.org/blog/oai-o3-pub-breakthrough.

159 See, e.g., Frazier, K., Rozenshtein, A.Z., & Salib, P.N. (2024, December 23). OpenAI's latest model shows AGI is inevitable. Now what? Lawfare. https://www.lawfaremedia.org/article/openai's-latest-model-shows-agi-is-inevitable.-now-what; see also, Allen, G.C. & Schwartz, A. (2025, January 13). AI diffusion framework – emergency podcast. Center for Strategic and International Studies. https://www.csis.org/analysis/ai-diffusion-framework-emergency-podcast.

160 Knoop, M. (2024, June 27). Introducing the ARC-AGI public leaderboard. https://arcprize.org/blog/introducing-arc-agi-public-leaderboard.

161 Chollet, F. (2019). On the measure of intelligence. ArXiv, 40. https://arxiv.org/abs/1911.01547v2.

162 Misunderstanding arose surrounding a post-hoc note by the ARC-AGI team specifying that OpenAI fine-tuned o3 on 75% of the public training set; ARC-AGI did not test the ARC-untrained model. Given that some data exposure is assumed on the semi-private evaluation, and the ARC-untrained model was not tested, it is not known whether OpenAI fine-tuned its model on leaked evaluation set data, thereby inflating o3's score.

163 In January 2025, information regarding OpenAI's involvement in Epoch AI's FrontierMath benchmark became widely shared, with the former funding the latter and requiring secrecy over the partnership until o3's unveiling while maintaining access to at least some test data (i.e., math problems). See, Meyer, D. (2025, January 21). 'Manipulative and disgraceful': OpenAI's critics seize on math benchmarking scandal. Fortune. https://fortune.com/2025/01/21/eye-on-ai-openai-o3-math-benchmark-frontiermath-epoch-altman-trump-biden/. This case is a cautionary tale and bears some (likely unintentional) resemblance to o3's testing on ARC-AGI.

164 Equally concerning is ARC-AGI's self-contradicting decision not to verify results for a system that scored a baseline performance on the public leaderboard of 83.75% - 85.75%, while nonetheless verifying o3's scores. See, Atreides, K. & Kelley, D. (2024). Solving the Abstraction and Reasoning Corpus for Artificial General Intelligence (ARC-AGI) AI benchmark with ICOM. ResearchGate, 1-30. http://dx.doi.org/10.13140/RG.2.2.32495.34727.

165 Chollet, F. [@fchollet]. (2024, December 30). It's doing CoT search [Post]. X. https://x.com/fchollet/status/1870174117342917041.

166 Weinberg, S. (1974). Reflections of a working scientist. Daedalus, 103(3), 40. https://www.jstor.org/stable/20024218

167 Garcez, A.d. & Lamb, L.C. (2023). Neurosymbolic AI: the 3rd wave. Artificial Intelligence Review, 56(11), 12389-12390. https://doi.org/10.1007/s10462-023-10448-w.

168 Trinh, T.H., Wu, Y., Le, Q.V., He, H. & Luong, T. (2024). Solving Olympiad geometry without human demonstrations. Nature, 625(7995), 476-482. https://doi.org/10.1038/s41586-023-06747-5.

169 Google DeepMind. (2024, July 25). AI achieves silver-medal standard solving International Mathematical Olympiad problems. https://deepmind.google/discover/blog/ai-solves-imo-problems-at-silver-medal-level/.

170 See, Marcus, G. (2024, July 28). AlphaProof, AlphaGeometry, ChatGPT, and why the future of AI is neurosymbolic. Marcus on AI. https://garymarcus.substack.com/p/alphaproof-alphageometry-chatgpt.

171 Marcus, G. (2024, October 9). Two Nobel Prizes for AI, and two paths forward. Marcus on AI. https://garymarcus.substack.com/p/two-nobel-prizes-for-ai-and-two-paths.

172 Jumper, J. et al. (2021). Highly accurate protein structure prediction with AlphaFold. Nature, 596(7873), 583-589. https://doi.org/10.1038/s41586-021-03819-2

173 Callaway, E. (2024, October 9). Chemistry Nobel goes to developers of AlphaFold AI that predicts protein structures. Nature. https://www.nature.com/articles/d41586-024-03214-7

174 Meta. (2022, November 22). Cicero. https://ai.meta.com/research/cicero/.

175 Meta Fundamental AI Research Diplomacy Team et al. (2022). Human-level play in the game of Diplomacy by combining language models with strategic reasoning. Science, 378(6624), 1067-1074. https://doi.org/10.1126/science.ade9097.

176 See, Marcus, G. & Davis, E. (2022, November 28). What does Meta AI's Diplomacy-winning Cicero mean for AI? Communications of the ACM. https://cacm.acm.org/blogcacm/what-does-meta-ais-diplomacy-winning-cicero-mean-for-ai/

177 Kautz, H.A. (2022). The third AI summer: AAAI Robert S. Engelmore memorial lecture. AI Magazine, 43(1), 118. https://doi.org/10.1002/aaai.12036

178 Silver, D. et al. (2017). Mastering the game of Go without human knowledge. Nature, 550(7676), 358. https://doi.org/10.1038/nature24270.

179 Marcus, G. (2018). Innateness, AlphaZero, and artificial intelligence. ArXiv, 6–9. https://doi.org/10.48550/arXiv.1801.05667.

180 Valmeekam, K., Stechly, K., Gundawar, A., & Kambhampati, S. (2024). Planning in strawberry fields: Evaluating and improving the planning and scheduling capabilities of LRM o1. ArXiv, 8–10, https://doi.org/10.48550/arXiv.2410.02162; see also, Gundawar, A., Valmeekam, K., Verma, M., & Kambhampati, S. (2024). Robust planning with compound LLM architectures: An LLM-Modulo approach. ArXiv, 1–21. https://doi.org/10.48550/arXiv.2411.14484.

181 Velasquez, A. (2022). Assured Neuro Symbolic Learning and Reasoning (ANSR). DARPA. https://www.darpa.mil/program/assured-neuro-symbolic-learning-and-reasoning.

182 DARPA. (2018). DARPA announces $2 billion campaign to develop next wave of AI technologies. https://www.darpa.mil/news-events/2018-09-07

183 National Science Foundation. (2023, August 1). NSF 23-610: National artificial intelligence (AI) research institutes: program solicitation. National Science Foundation. https://nsf-gov-resources.nsf.gov/solicitations/pubs/2023/nsf23610/nsf23610.pdf?VersionId=DtbAJgpPY438dSJD6rA.55zjuXLlgvnS: 12–13.

184 National Science Foundation. (2023, August 1). NSF 23-610: National artificial intelligence (AI) research institutes: program solicitation. National Science Foundation. https://nsf-gov-resources.nsf.gov/solicitations/pubs/2023/nsf23610/nsf23610.pdf?VersionId=DtbAJgpPY438dSJD6rA.55zjuXLlgvnS: 13.

185 National Science Foundation. (2023, August 1). NSF 23-610: National artificial intelligence (AI) research institutes: program solicitation. National Science Foundation. https://nsf-gov-resources.nsf.gov/solicitations/pubs/2023/nsf23610/nsf23610.pdf?VersionId=DtbAJgpPY438dSJD6rA.55zjuXLlgvnS: 12.

186 National Science Foundation. (2021, June 25). EAGER: advancing neuro-symbolic AI with Deep Knowledge-infused learning. National Science Foundation. https://www.nsf.gov/awardsearch/showAward?AWD_ID=2133842&HistoricalAwards=false.

187 Hagos, D.H. & Rawat, D.B. (2024). Neuro-Symbolic AI for military applications. ArXiv, 4. https://doi.org/10.48550/arXiv.2408.09224.

188 Gaur, M. & Sheth, A. (2024). Building trustworthy NeuroSymbolic AI systems: Consistency, reliability, explainability, and safety. AI Magazine, 45(1), 139–155. https://doi.org/10.1002/aaai.12149.

189 Wu, D. (2024, September 6). TSMC's Arizona trials put plant productivity on par with Taiwan. Bloomberg. https://www.bloomberg.com/news/articles/2024-09-06/tsmc-s-arizona-trials-put-plant-productivity-on-par-with-taiwan?srnd=undefined

190 Varadarajan, R., Koch-Weser, I., Richard, C., Fitzgerald, J., Singh, J., Thornton, M., Casanova, R., & Isaacs, D. (2024). Emerging resilience in the semiconductor supply chain. Boston Consulting Group & Semiconductor Industry Association, https://www.semiconductors.org/wp-content/uploads/2024/05/Report_Emerging-Resilience-in-the-Semiconductor-Supply-Chain.pdf: 4.

191 Sheth, A., Roy, K., & Gaur, M. (2023). Neurosymbolic artificial intelligence (Why, what, and how). IEEE Intelligent Systems, 38(3), 56–62. https://doi.org/10.1109/MIS.2023.3268724.

192 See, Donlon, J.J. (2024). The National Artificial Intelligence Research Institutes program and its significance to a prosperous future. AI Magazine, 45(1), 6. https://doi.org/10.1002/aaai.12153.

193 Donlon, J.J. (2024). The National Artificial Intelligence Research Institutes program and its significance to a prosperous future. AI Magazine, 45(1), 11. https://doi.org/10.1002/aaai.12153.

194 Stewart, N. (2024). Funding for the future: The case for federal R&D spending [White paper]. Special Competitive Studies Project, https://www.scsp.ai/wp-content/uploads/2024/01/RD-White-Paper-2.pdf: 5.

195 See, Zegart, A. (2024, August 20). The crumbling foundations of American strength. Foreign Affairs. https://www.foreignaffairs.com/united-states/crumbling-foundations-american-strength-amy-zegart.

196 Soliman, M. & Carchidi, V. (2024, September 23). Re-Balancing the strategy of tech containment. Foreign Policy Research Institute. https://www.fpri.org/article/2024/09/re-balancing-the-strategy-of-tech-containment/; see also, Carchidi, V & Soliman, M. (2024). The role of the Middle East in the US-China race to AI supremacy. Middle East Institute. https://www.mei.edu/publications/role-middle-east-us-china-race-ai-supremacy: 36–38.

197 Fast Track Action Subcommittee on Critical and Emerging Technologies of the National Science and Technology Council. (2024). Critical and emerging technologies list update. Executive Office of the President of the United States. https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf, 4.

Contact

For media inquiries, email media@newlinesinstitute.org

To submit a piece to the New Lines Institute, email submissions@newlinesinstitute.org

For other inquiries, send an email to info@newlinesinstitute.org

1660 L St. NW, Suite 450
Washington, D.C., 20036

(202) 800-7302

Connect With Us

@newlinesinst | @New Lines Institute for Strategy and Policy | Subscribe | Sign up

NEW LINES INSTITUTE
FOR STRATEGY AND POLICY