II. Securing Vital U.S. Technological Advantages

Advanced technology translates directly into military and economic power, and further provides leading nations with the ability to shape international norms and domestic governance practices. Sustaining America's technological edge will therefore be vital to realizing a free and open Indo-Pacific. Fortunately, the United States retains a number of advantages in the technological competition with China: world-class universities and research institutes, leading technology companies, a vibrant venture capital and start-up ecosystem, and a long history of rewarding innovation. America has also benefited profoundly from being a place where people from around the world want to work and live.

Yet, largely due to choices in Washington and Beijing, America's position as the global technology leader is under threat. U.S. expenditures on research and development have stagnated for decades as a share of gross domestic product (GDP). In the meantime, China has quadrupled its spending and is on the brink of surpassing the United States in total investments in this area.[25] Already, the results are showing: China is now a global powerhouse in a number of strategic technologies, equal to or ahead of the United States in critical areas such as quantum computing, artificial intelligence, and genomics.[26] If current trends continue, the downstream military, economic, and political consequences could tip the scales toward China's vision of regional order in the Indo-Pacific.

To keep apace, Washington will have to do more to reinvigorate American technological leadership. The U.S. government should set ambitious national goals for public and private spending on research and development, while bolstering human capital and high-skilled immigration. Relying on competitive, market-oriented principles—and avoiding a heavy-handed industrial policy in which the government picks winners and losers—Washington should provide resources and data to defend and advance key areas of U.S. competitive advantage, including artificial intelligence and semiconductors.

As it reinvigorates its innovation base at home, the United States will have to be more vigilant in protecting key U.S. technologies. Recent legislative efforts to enhance U.S. investment screening and export controls are a good start and must be followed through. But more comprehensive efforts are still needed to address China's harmful and illicit practices of forced technology transfer, academic and commercial espionage, and intellectual property theft. Washington will have to establish a more productive and collaborative relationship with U.S. businesses and universities. It will also be necessary to augment resources for counterespionage investigations and visa screening, as well as a demonstrated willingness and ability to retaliate against Chinese firms and individuals that benefit from technology theft.

Critically, going it alone will be insufficient for the United States, both because of China's economies of scale and because unilateral defensive measures will be ineffective if Beijing can easily exploit other advanced economies. Washington should lead on establishing a new international body of democratic powers to coordinate on technology policy and develop cooperative solutions to combating China's anti-competitive practices.

Sustaining U.S. technological advantages will also require the United States to be more proactive internationally in setting new rules around emerging technologies. Active U.S. participation in international standards-setting bodies will be essential. Meanwhile, the United States can lead efforts in the Indo-Pacific and globally to codify norms for the use of emerging technologies. This should include detailed discussions with Beijing over the future of artificial intelligence.

Recommendations for U.S. Policy

BOLSTER AMERICA'S INNOVATION ENGINE

Increase investments in research and development in the United States

The federal government plays a unique and critical role in America's innovation ecosystem: Government research and development (R&D) spending spurs private-sector investments,[27] and the U.S. government remains the largest funder of basic research, which is foundational to game-changing technological achievements.[28] Notably, U.S. government investments in the 1960s and 1970s in semiconductors, the global positioning system (GPS), and the early internet paved the way for the digital world of today. Yet, while private-sector R&D investments have steadily increased in the United States, federal government spending has declined as a percentage of GDP from approximately 1.2 percent in 1976 to around 0.7 percent in 2018.[29]

To sustain another generation of technology leadership, the United States should increase federal R&D spending to 1.2 percent of GDP, matching levels in the 1970s. To execute such a significant increase, funding should increase gradually through existing organizations (Department of Defense, National Institutes of

Health, and Department of Energy, among others).[30] The White House Office of Science and Technology Policy (OSTP) should lead an interagency process, in consultation with external scientific advisors, to identify key strategic technologies for focused investment, such as artificial intelligence, microelectronics, quantum computing, wireless networking, synthetic biology, advanced manufacturing, health, energy, or other areas. As a bipartisan response to the intensifying technology competition with China, Congress could jump-start a new era of federal investment by passing a comprehensive appropriations bill.

In addition to federal spending, the United States should increase total national (public and private) R&D expenditures to keep pace with other leading technology nations. South Korea and Israel, for example, spend greater than 4.5 percent of GDP on R&D, while total U.S. public and private R&D spending in 2017 was only 2.8 percent.[31] Using tax incentives to spur private-sector investment, the United States should establish a goal of bringing total (public and private) R&D spending to 4 percent of GDP by 2030.

Accelerate U.S. innovation in artificial intelligence through standards-setting, metrics, and horizon-scanning

Artificial intelligence and machine learning are rapidly developing fields, fueled by exponential growth in data and computing processing power ("compute"). The federal government has an important role in advancing U.S. competitiveness in these vital areas, even while much of the innovation will remain private-sector-driven.[32] Government-led standards-setting is critical for enabling innovation, as are metrics for tracking progress and incentivizing research against specific problems.[33] The National Institute of Standards and Technology (NIST) and the Office of Science and Technology Policy should establish an interagency subcommittee for AI standards and measurement, under the National Science and Technology Council (NSTC) Select Committee on AI.

Long-term analysis on future trends and threats is also critical to understanding rapid technology development and preventing harmful technological surprises. Such efforts can help national security leaders anticipate potential future challenges, such as detection-resistant "deep fakes," and prepare mitigation measures in advance. The departments of Commerce, Defense, and Homeland Security, along with the intelligence community, should collaborate with OSTP to analyze global AI trends and anticipate future challenges.

Support U.S. innovation in artificial intelligence and machine learning by increasing the availability of government data and computing resources

The U.S. government should take steps to increase the availability of data and compute, both of which are key inputs for research and innovation on AI and machine learning. This is particularly important for university researchers, who may lack the financial resources available to private-sector AI researchers. OSTP and the Office of Management and Budget (OMB) should build on Project Open Data by expanding the number of open-source high-quality datasets, an important asset for machine learning.[34] To increase compute resources for researchers, Congress should boost funding for the National Science Foundation's Enabling Access to Cloud Computing Resources for CISE (Computer and Information Science and Engineering) Research and Education program and the Exploring Clouds for Acceleration of Science (E-CAS) project.[35]

Forge an alliance innovation base

To keep pace with China's military-civil innovation complex, the United States should develop deeper technology cooperation with key allies. This could take multiple forms. For example, DoD could expand existing mechanisms for quick-fire international seed projects. More ambitiously, the United States could stand up a "Freedom's Foundry" that would bring together U.S. innovators and entrepreneurs with counterparts from allied countries to develop novel technologies—even new companies—around specific national security themes. With joint funding from participating governments and the private sector, these efforts could intersect with commercial market opportunities.

PROTECT CRITICAL U.S. TECHNOLOGICAL ADVANTAGES

Secure semiconductor supply chains

Along with artificial intelligence, U.S. technological advantages in semiconductors will be critical to advancing U.S. competitiveness in the Indo-Pacific. Although the United States is a global leader in semiconductor design—with U.S. headquartered firms accounting for roughly half of the global market—most fabrication occurs overseas.[36] This heavy reliance on overseas production presents substantial risks to vital U.S. economic and security interests.[37] As a result, the United States should develop trusted semiconductor suppliers for

defense and intelligence applications in order to ensure chips are free from potential tampering by adversaries and are not easily subject to disruption. Washington can also collaborate with key allies to establish an international fabrication consortium to diversify semiconductor fabrication.

On the order of $10 billion to $20 billion, the costs of establishing a new foundry present a major challenge to diversifying semiconductor supply chains, making onshoring prohibitively expensive even with potential government subsidies.[38] Additionally, the U.S. military and intelligence community have special needs for security that go above and beyond what is available in commercial facilities, yet they lack the scale of demand to make a purely government-dedicated foundry profitable.[39] DoD and the intelligence community should therefore explore novel approaches for public-private partnerships with U.S. companies to build the capability for trusted design, fabrication, packaging, and testing. Additionally, the United States should explore establishing an international fabrication consortium with allies to share the costs of building new semiconductor foundries that can ensure a trusted and diverse supply chain. As a starting point, member nations of the consortium should include the global leaders in semiconductor manufacturing equipment: the United States, Japan, and the Netherlands.

Establish multilateral export controls on semiconductor manufacturing equipment and increase federal funding for next-generation hardware

The United States has a major global lead in semiconductor design and should enact multilateral export controls, in concert with allies and partners, to protect its current technological advantage in hardware. This is among the most important actions the United States can take to protect its competitive edge in artificial intelligence. Furthermore, export controls should be coupled with increased federal R&D funding for next-generation hardware to ensure continued U.S. leadership.

China is heavily dependent on imports of foreign-manufactured semiconductors to meet internal demand. As part of its industrial policy to seize technological leadership from the United States, China is looking to reduce its reliance on foreign chips by ramping up domestic semiconductor production.[40] To accomplish this goal, China will need foreign imports of semiconductor manufacturing equipment (SME), which comprises the equipment and tools needed to establish a chip fabrication facility, or foundry. The global SME market is highly centralized, with the United States, Japan, and the Netherlands accounting for 90 percent.[41]

While export controls on semiconductors themselves should be rare and targeted, such as the action against Huawei and a handful of other companies linked to the Chinese military, the United States should enact broad restrictions on sales of SME to China to sustain the U.S. advantage in hardware. In parallel, the Commerce and State departments should work with key allies and partners (the Netherlands, Japan, South Korea, and Singapore) to establish multilateral export controls on SME, thereby further restricting sales to China.

It is true that SME export controls would reduce profits from sales in China that U.S. companies might have reinvested in R&D.[42] Nevertheless, the imperative of protecting U.S. technological advantage makes this a necessary expense, and the U.S. government can increase R&D funding in next-generation chip design, fabrication, and packaging to help fill the gap and ensure continued U.S. leadership in semiconductors.

Diversify sources of rare earth minerals

The United States must also secure the underlying raw materials behind digital technologies. Rare earth minerals, in particular, are essential for electronics, missile guidance systems, and military platforms such as fighter aircraft and submarines.[43] Yet China has near-complete control over the U.S. rare earths supply chain: As of 2018, China supplied 80 percent of U.S. rare earth imports and much of the chemical intermediates and mineral concentrates needed to process what was imported from Estonia, France, and Japan.[44] China further controls at least 85 percent of global rare earth processing capacity.[45]

The U.S. government can take a number of important steps to help reduce U.S. reliance on China for rare earths. The U.S. Department of Defense, for instance, has already initiated efforts to expand mining and processing of rare earths outside China, including in Australia.[46] To reduce dependence on overseas suppliers more generally, Congress should ensure funding for the Department of Commerce's plan to reinvigorate mining and processing of rare earths in the United States,[47] and Department of Energy research into and scaling of rare earth recycling from consumer products, which can stretch existing U.S. supplies.[48] Finally, Congress should support Department of Energy efforts to develop artificial substitutes, which have proved capable of reducing dependence on rare earths altogether.[49]

Expand export controls based on end use for certain products sold to China

To ensure U.S. technology does not enable China's malign behavior, the U.S. government should develop additional tools beyond existing restrictions on military exports. To that end, the U.S. Commerce Department should undertake the development of a new export control regulation that would restrict the sale of both key U.S.-origin products and key foreign-origin products developed by U.S. companies and their subsidiaries overseas to be used for certain end uses in China, including those that infringe on internationally accepted human rights standards, enable surveillance or cyberespionage, and are involved in domestic security activities.

Creating a new end-use-based control regime would require rigorous consideration by the U.S. government, as well as shifts in compliance protocols by a number of U.S. private-sector exporters. The Commerce Department should develop end-use-based controls in consultation with the U.S. private sector, engaging in a full administrative rulemaking process to seek feedback from national security professionals and industry.

COUNTER ILLICIT TECHNOLOGY TRANSFER

Ensure sufficient resources for counterespionage investigations

China poses a major counterintelligence threat to the United States, accounting for 90 percent of all Department of Justice (DoJ) espionage cases involving a state actor between 2011 and 2018.[50] The DoJ has begun ramping up efforts to counter this threat, with roughly 1,000 FBI investigations underway involving attempted intellectual property theft by China.[51] Moreover, the DoJ established a new China Initiative in 2018 to increase outreach to universities and business, interagency coordination, and investigation of Chinese investments and influence operations, among other activities.

As these efforts move forward, Congress should provide the FBI and DoJ with sufficient resources—particularly for Chinese language skills and scientific and technical expertise—to ensure there is adequate capacity to carry out thorough counterespionage investigations. FBI Director Christopher Wray has identified Mandarin skills as a gap for the FBI,[52] and insufficient technical knowledge has at times been an obstacle in prior cases.[53]

Develop better collaboration between U.S. law enforcement and universities

Universities have a strong interest in preventing countries such as China from unfairly exploiting research by their faculty and students, while also protecting core values of academic freedom and fostering transnational research. As universities and the FBI are both implementing measures to address academic espionage concerns on campuses, greater dialogue is urgently needed between investigators and academics to better understand the scope of the problem and work together on possible solutions.[54] Fortunately, some positive steps are already underway under the auspices of OSTP and the academic community.[55] More should be done, however, to ensure greater coordination between universities and the national security community on this important topic. Such action should include the reestablishment of the National Security Higher Education Advisory Board, which was established to build lines of communication and cooperation between universities and the national security community on counterintelligence threats, among other issues.[56]

Improve visa screening for espionage risks

The United States benefits greatly from foreign students at U.S. universities, many of whom stay for work and support the U.S. economy.[57] These academic exchanges are a significant source of strength for the United States and should be protected. Guided by that principle, Congress should nevertheless work with the State Department, FBI, and intelligence community to develop enhanced criteria for visa screening to identify individuals from China who pose heightened espionage risks.[58] Possible risk factors could include whether an individual comes from a university with ties to the PLA or cites highly specific research interests relating to defense technologies.[59]

Recently proposed U.S. legislation includes both actor-based and technology-based approaches to improve visa screening. The People's Liberation Army (PLA) Visa Security Act would prohibit F or J visas for PLA-employed, -funded, or -sponsored individuals, and the Protect Our Universities Act of 2019 would mandate background screening of students seeking to work on "sensitive research projects."[60] Both proposals are sensible measures and should be implemented, but broader screening could still be required. This is in

part because many important technology areas, such as AI, have both commercial and military applications. Beyond evident military-specific research projects, more stringent screening is also needed for a wider range of dual-use technologies.[61]

Expand sanctions authorities to cut off from the U.S. market and financial system Chinese firms that steal U.S. technology

The United States has failed to sufficiently penalize Chinese companies known to be benefiting from stolen U.S. technology. Going forward, Chinese firms that engage in significant intellectual property (IP) theft and other anti-competitive behavior should be cut off from the U.S. market and the U.S. financial system. Existing U.S. sanctions authorities allow the executive branch to sanction foreign companies, including Chinese ones, that engage in cyber-enabled IP theft, but these authorities do not fully capture other types of IP theft, such as by corporate insiders. The U.S. Treasury Department, working with the Commerce Department and the State Department, should lead in developing and enforcing a new regime to enable sanctions against the full range of IP theft.

Include more People's Liberation Army-linked companies on the export regime Entity List

China engages in a systematic and multifaceted campaign of both licit and illicit technology transfer to acquire access to advanced U.S. technology and repurpose it for the Chinese military.[62] Although U.S. law generally prohibits the sale of U.S. products to the PLA and other military end users in China, Beijing's promotion of military-civil fusion means that civilian entities in China that are closely linked to the PLA can still legally purchase U.S.-made products.[63] This problem is exacerbated by the fact that many cutting-edge technologies, such as AI, are dual-use, with both valuable military and commercial applications.

The U.S. government has made some progress in using existing export control authorities to restrict the export of U.S. products to Chinese entities that are tied to the PLA. For example, in June 2019, the Commerce Department added five PLA-linked supercomputing organizations to the Entity List, which prohibits the sale or provision of U.S.-made products to the designated organizations. Expanding the list of named PLA-linked entities barred from receiving U.S. products and prohibiting visas for PLA-sponsored individuals will help limit proliferation of U.S. technology to the PLA.

To that end, the Commerce Department and Department of Defense should lead an interagency process to compile an extensive, publicly releasable, and regularly updated list of PLA-linked entities in China and add them to the Commerce Entity List. (An initial such effort is reportedly underway.[64]) In addition to curbing unwanted technology transfer to the PLA, this would help to expose China's military-civil fusion strategy and make it riskier to invest in companies that work with the PLA. Finally, the United States should prohibit F and J visas for PLA-employed, -funded, or -sponsored individuals.[65]

LEAD ON DEVELOPING NEW INTERNATIONAL RULES, NORMS, AND STANDARDS FOR EMERGING TECHNOLOGIES

Create a new grouping of advanced democracies to coordinate on technology policy

U.S. efforts to spur innovation and protect key areas of competitive advantage are far more likely to succeed if major elements of U.S. policy are coordinated and jointly implemented with allies and partners. Multilateral cooperation among like-minded countries would serve to amplify the effectiveness of the measures across a range of areas, including R&D, supply chain diversity and security, standards-setting, multilateral export controls, and countering illiberal uses of technology. To achieve the necessary level of coordination and collaboration, the United States should lead the creation of a new multilateral grouping on technology policy.[66]

The purpose of this new body would be to coordinate multinational technology policy to protect and advance key areas of competitive technological advantage, and to promote collective norms and values around the use of emerging technologies. Leading liberal-democratic technological and economic powers—including Australia, Canada, France, Germany, Japan, the Netherlands, South Korea, and the United Kingdom, among others—would comprise the group's core membership. This new organization could cooperate on 5G, semiconductors, AI, cybersecurity, internet of things, and other significant technologies. Increased information sharing and cooperation could help nations develop cooperative solutions for technology leadership and defend against intellectual property theft, espionage, and other unfair trade practices that harm competition and distort free and fair markets.

Engage more proactively in multilateral bodies that set technology standards

The United States has a strong national security interest in the development of international technical standards, which are critical for shaping how technology is adopted around the world for 5G wireless, artificial intelligence, internet of things, and other emerging technologies.[67] However, while the U.S. government has been insufficiently engaged,[68] China has become increasingly proactive in international bodies, elevating standards-setting as a major priority with its "China Standards 2035" plan.[69]

Working in partnership with U.S. industry leaders, the U.S. government should increase its participation in international technology standards-setting bodies, including the 3rd Generation Partnership Project (3GPP), International Telecommunication Union (ITU), and International Organization for Standardization (ISO), among others.[70] To accomplish this goal, OSTP should establish an interagency working group on international technology standards, bringing together the departments of State, Commerce, Justice, and Defense; the U.S. intelligence community; and the NIST to coordinate U.S. government action. This interagency group should also increase engagement with U.S. industry leaders, including information sharing on technical standards and Chinese efforts to exert political influence within international standards-setting bodies.[71] Participation in standards-setting bodies should be explicitly exempted from export controls so U.S. companies and government officials can help shape international standards even if prohibited Chinese entities are also participating.

Lead internationally and engage with China on developing norms and principles for the use of emerging technologies

The United States should work with allies and partners to establish and export norms for using emerging technologies, including AI and biotechnology. U.S. officials should also engage China where there may be opportunities for norm development. The United States has a vested interest in helping to shape, to the extent possible, how China uses technology, which will have significant global implications. A number of Chinese actors have already released AI "principles" documents, similar to those released by businesses, governments, and nongovernmental organizations around the globe. These principles indicate some degree of norm transfer to China.

Continuing to develop formal norms such as the AI principles the Organisation for Economic Co-operation and Development (OECD) recently adopted is valuable, but equally important will be demonstrating responsible use in applications at home and abroad. The dynamic interplay in democratic nations between civil society, nongovernmental organizations, companies, the government, and a free press over how to use technology while balancing competing interests sets an important example for other nations and stands in stark contrast to the illiberal use of technology by autocratic regimes.