American Edge Project:

The Decisive Decade: A National Security Policy Designed To Help America Win The Tech Race Against China

/edge

AMERICAN EDGE PROJECT

/edge
AMERICAN EDGE PROJECT

The Decisive Decade: A National Security Policy Designed To Help America Win The Tech Race Against China

June 2023

Introduction

Over the past four decades, technological innovation has produced unprecedented societal benefits that would have been unimaginable only one century ago. Led by the United States, the world's democracies have been at the forefront of developing and deploying technological tools to address some of society's greatest challenges, from curing disease and mitigating climate change to expanding access to education and improving connectivity. Most recently, leaps in artificial intelligence (AI) have showcased its potential to reshape entire sectors of the economy across the globe.

Yet, like any tool, technology can also be used for perverse purposes. The United States and other "techno-democracies" find themselves in a competition with "techno-autocracies" like the People's Republic of China (PRC) and Russia that routinely use technology to surveil, censor, and manipulate public opinion both at home and abroad. Techno-autocracies are even using technology to defy inalienable rights of freedom and territorial sovereignty, relying on technological advancements to repress religious minorities in Xinjiang, threaten the independence of Taiwan, and wage war on the people of Ukraine.

Whether China, Russia, and the techno-autocracies of tomorrow succeed in creating a new global order that promotes their authoritarian values will hinge on their race with the United States and like-minded nations to lead concerning the technologies of tomorrow. The outcome of that race will have profound implications for the United States and its global partners' national security, economic prosperity, and capacity to set technological standards and norms that support democratic values and deter digital authoritarianism.

The following policy platform builds on the American Edge Project's inaugural national security policy issued in February 2021 and provides a roadmap for ensuring the United States maintains its technological edge over techno-autocracies. The first "pillar" focuses on *accelerating America's ability to innovate* by investing heavily in emerging technologies and cloud computing infrastructure that will underpin competition among great powers in the future, as well as foster greater private sector research and development here at home. The second pillar discusses *strengthening global technology alliances* and working with our allies and partners to secure supply chains and data flows. The third and final pillar addresses *defending against digital authoritarianism*, including practicing strategic decoupling from China, empowering American technology companies to continue to act as our first line of defense against cyberattacks from adversaries, and countering disinformation and election interference.

Pillar One: Accelerating America's Ability to Innovate

The United States and China are in a race for technological superiority. While the United States maintains a slight technological edge in many of the emerging technologies that are critical to continued U.S. prosperity and remains a global leader in cloud computing, a number of studies show our lead is narrowing quickly or has already disappeared. A recent report[1] published by the respected Australian Strategic Policy Institute (ASPI) found that China has surged ahead of America in 37 of 44 categories of critical technologies and that, in some cases, China is approaching a near-dominant position in that technology.

"China has surged ahead of America in 37 of 44 categories of critical technologies and that, in some cases, China is approaching a near-dominant position in that technology."

To reclaim and maintain the U.S. innovation edge, policymakers must aggressively invest in the emerging technologies that will determine the future of competition between great powers, create incentives for technology companies to further invest in research and development in the United States, and bolster cloud computing cybersecurity to protect our digital infrastructure from foreign adversaries.

Boost Public Sector Investment in Emerging Technologies

The United States is competing against China to advance and define the emerging technologies foundational to the 21st Century. Winning that race will be essential to maintaining U.S. national and economic security, as well as that of its partners. In the wrong hands, an adversary's advantage in quantum technologies, AI, advanced robotics, advanced power supplies, advanced hypersonics, and space technologies could pose significant military threats to the U.S. on land, air, and water, and in space, and break modern encryption protocols to expose sensitive U.S. data, and violate consumer privacy.

Additionally, widespread deployment of Chinese telecom infrastructure, subsea cable networks, and financial technology would allow Beijing to scale state espionage, control the flow of information to suit its policy priorities, and exert disproportionate influence around international standard setting.[2]

[1] Gaida, Jamie, Jennifer Wong Leung, Stephan Robin, and Danielle Cave, "ASPI's Critical Technology Tracker – AUKUS Updates," Australian Policy Institute, March 2023, https://www.aspi.org.au/report/critical-technology-tracker.

[2] Neaher, Giulia, David Bray, Julian Mueller-Kaler, and Benjamin Schatz, "Standardizing the Future: How Can the United States Navigate the Geopolitics of International Technology Standards," Atlantic Council, October 2021,

Similarly, biotechnology is another emerging technology where, without U.S. leadership, techno-autocracies could pursue dangerous uses of genomics and gene editing. Thirdly, China's efforts to corner the rare earth marketplace and control the manufacturing of critical hardware necessary for technology, communication, innovation and infrastructure pose a threat to technological advancement and economic growth. Finally, advanced semiconductors, the cornerstone of many of the technologies above, are critical to the development of advanced military weapons, sensors, and encryption.

China is investing trillions to outcompete the United States, including through its military-civil fusion (MCF) strategy that aims to enable it to develop the most technologically advanced military in the world by eliminating barriers between its civilian research and commercial sectors and its military and defense industrial sectors. Technologies targeted under China's MCF strategy include emerging technologies, such as artificial intelligence, quantum computing, advanced aerospace technology, and semiconductor technology.[3] More recently, China's National People's Congress approved the State Council Institutional Reform Plan to restructure the Chinese Science and Technology Ministry to align with PRC priorities in technology innovation, invest in basic research, and translate gains into practical applications.[4] Much of the Chinese Communist Party's (CCP) rhetoric surrounding the reform plan has focused on boosting China's self-reliance in key technology areas, suggesting it will redouble its efforts to advance disruptive technologies and raising concerns that China could accelerate its pace of innovation via state support.

Their efforts are paying off. As studies indicate, the U.S. maintains a lead in **biotechnology** and **advanced semiconductors**,[5] **quantum computing and sensing**,[6] **space technologies**,[7] and **subsea cable networks.** The United States is at parity with China in **artificial intelligence**[8] and squarely losing to China in **advanced power supplies,** such as supercapacitors and electric batteries, **quantum communications**,

https://www.atlanticcouncil.org/in-depth-research-reports/report/standardizing-the-future-how-can-the-united-states-navigate-the-geopolitics-of-international-technology-standards/.

[3] U.S. Department of State, "Military-Civil Fusion and the People's Republic of China," May 2020, https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

[4] Feng, Emily, "China is Restructuring Key Government Agencies to Outcompete Rivals in Tech," *NPR*, March 2023, https://www.npr.org/2023/03/07/1161591936/china-government-restructure-tech-competition.

[5] Allison, Graham, Kevin Klyman, Karina Barbesino, and Hugo Yen, "The Great Teach Rivalry: China vs. the U.S.," Harvard Kennedy School Belfer Center for Science and International Affairs, December 2021, https://www.belfercenter.org/sites/default/files/GreatTechRivalry_ChinavsUS_211207.pdf.

[6] RAND Corporation, "An Assessment of the U.S. and Chinese Industrial Base in Quantum Technology," 2022, https://www.rand.org/pubs/research_reports/RRA869-1.html.

[7] Office of the Director of National Intelligence, "Chinese Space Activities Will Increasingly Challenge US Interests Through 2030," April 2021, https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Chinese-Space-Activities-through-2030--2022.pdf.

[8] Smith, Craig, "China's AI Implementation is Edging Ahead of the US," *Forbes*, January 2023, https://www.forbes.com/sites/craigsmith/2023/01/14/chinas-ai-implementation-is-edging-ahead-of-the-us/?sh=53e3b1b12dfb.

6G[9] and **financial technology**.[10] Additionally, the United States is losing to both China and Russia in nuclear-capable **hypersonic weapons**.[11] And by some measures, the United States is also behind in **advanced robotics**, **quantum sensing**, and key aspects of biotechnology, such as **synthetic biology**.[12]

Even in areas where the United States is leading, the scales could tip further in China's favor as it doubles down on technological innovation. China's Baidu unveiled its first quantum computer in August 2022, bringing it one step closer to a fault-tolerant quantum computer. The CCP is providing state support to telecommunications companies to lay down cables along new, previously inaccessible routes that avoid geopolitical hot spots.[13] And even in space, the U.S. intelligence community assesses that, by 2030,

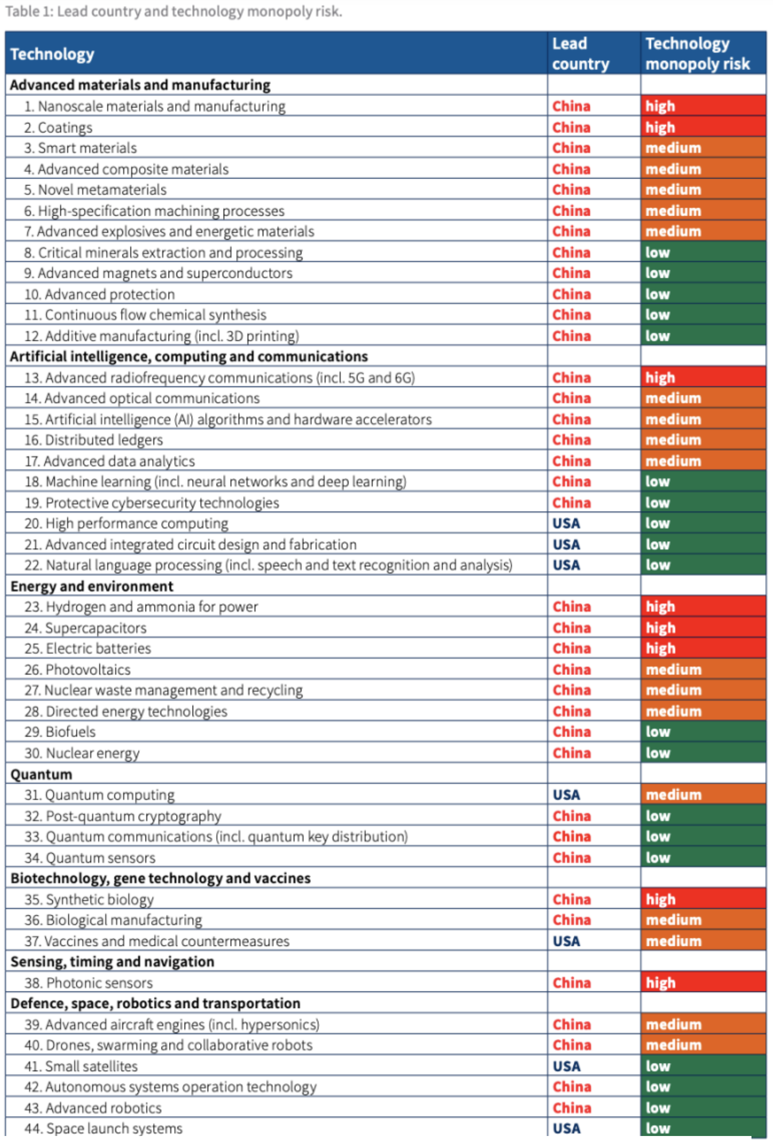


Table 1: Lead country and technology monopoly risk.

Technology	Lead country	Technology monopoly risk
Advanced materials and manufacturing		
1. Nanoscale materials and manufacturing	China	high
2. Coatings	China	high
3. Smart materials	China	medium
4. Advanced composite materials	China	medium
5. Novel metamaterials	China	medium
6. High-specification machining processes	China	medium
7. Advanced explosives and energetic materials	China	medium
8. Critical minerals extraction and processing	China	low
9. Advanced magnets and superconductors	China	low
10. Advanced protection	China	low
11. Continuous flow chemical synthesis	China	low
12. Additive manufacturing (incl. 3D printing)	China	low
Artificial intelligence, computing and communications		
13. Advanced radiofrequency communications (incl. 5G and 6G)	China	high
14. Advanced optical communications	China	medium
15. Artificial intelligence (AI) algorithms and hardware accelerators	China	medium
16. Distributed ledgers	China	medium
17. Advanced data analytics	China	medium
18. Machine learning (incl. neural networks and deep learning)	China	low
19. Protective cybersecurity technologies	China	low
20. High performance computing	USA	low
21. Advanced integrated circuit design and fabrication	USA	low
22. Natural language processing (incl. speech and text recognition and analysis)	USA	low
Energy and environment		
23. Hydrogen and ammonia for power	China	high
24. Supercapacitors	China	high
25. Electric batteries	China	high
26. Photovoltaics	China	medium
27. Nuclear waste management and recycling	China	medium
28. Directed energy technologies	China	medium
29. Biofuels	China	low
30. Nuclear energy	China	low
Quantum		
31. Quantum computing	USA	medium
32. Post-quantum cryptography	China	low
33. Quantum communications (incl. quantum key distribution)	China	low
34. Quantum sensors	China	low
Biotechnology, gene technology and vaccines		
35. Synthetic biology	China	high
36. Biological manufacturing	China	medium
37. Vaccines and medical countermeasures	USA	medium
Sensing, timing and navigation		
38. Photonic sensors	China	high
Defence, space, robotics and transportation		
39. Advanced aircraft engines (incl. hypersonics)	China	medium
40. Drones, swarming and collaborative robots	China	medium
41. Small satellites	USA	low
42. Autonomous systems operation technology	China	low
43. Advanced robotics	China	low
44. Space launch systems	USA	low

Table 1, "Policy Brief: ASPI's Critical Technology Tracker: The Global Race for Future Power."

[9] Australian Strategic Policy Institute, "ASPI's Critical Technology Tracker: The Global Race for Future Power," February 2023, https://www.aspi.org.au/report/critical-technology-tracker.

[10] Chorzempa, "How China Leapfrogged Ahead of the United States in the Fintech Race," Peterson Institute for International Economics, April 2018, https://www.piie.com/blogs/china-economic-watch/how-china-leapfrogged-ahead-united-states-fintech-race.

[11] Demirjian, Karoun, "U.S. Touts Progress in Hypersonic Arms Race with China, Russia," *The Washington Post*, July 2022, https://www.washingtonpost.com/national-security/2022/07/19/hypersonic-missile-pentagon-china-russia/.

[12] Australian Strategic Policy Institute, "ASPI's Critical Technology Tracker."

[13] Goodman and Wayland, "Securing Asia's Subsea Network: U.S. Interests and Strategic Options."

China will achieve world-class status in all but a few space technology areas.[14]

> **“The United States must urgently and aggressively invest in these emerging technologies to avoid losing its technological edge over China, forsaking trillions in economic opportunity and surrendering its advantage in military and intelligence-gathering capabilities.”**

The 2022 U.S. National Security Strategy states that, “in the competition with the PRC, as in other arenas, it is clear that the next ten years will be the decisive decade.”[15] The United States must urgently and aggressively invest in these emerging technologies to avoid losing its technological edge over China, forsaking trillions in economic opportunity and surrendering its advantage in military and intelligence-gathering capabilities. Since the fall of the Soviet Union, U.S. technological innovation has become a distinctly private sector enterprise rather than a government responsibility, with the private sector spending more than 3.5 times more research and development dollars than the public sector.[16] It is imperative that the U.S. government resume a more active role, increasing public sector investment in emerging technology research and development, as well as striking national security partnerships with and providing incentives for the private sector to invest in research and development and grow the U.S. industrial base (*see “Foster Private Sector Innovation”*).

Despite the slew of competing policy priorities facing lawmakers, the United States must prioritize making these investments today to maintain its technological competitiveness tomorrow. The bipartisan CHIPS and Science Act of 2022 was a step in the right direction, making record investments in domestic semiconductor manufacturing and science and technology programs. Although there were concerns about the bill, at a minimum, it sent an important signal about the federal government's commitment to support emerging technologies. Yet the legislation only passed once the United States was already at a disadvantage, facing severe chip shortages that cost the U.S. economy hundreds of billions of dollars.[17] Lawmakers must avoid repeating the same mistake when it comes to other emerging technologies with global significance.

[14] Office of the Director of National Intelligence, “Chinese Space Activities Will Increasingly Challenge US Interests Through 2030,” October 2022, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2329-chinese-space-activities-will-increasingly-challenge-u-s-interests-through-2030.

[15] The White House, “2022 National Security Strategy,” October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

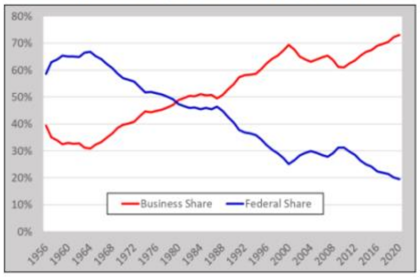
[16] West, Darrell, “R&D for the Public Good: Ways to Strengthen Societal Innovation in the United States,” Brookings Institution, October 2022, https://www.brookings.edu/research/rd-for-the-public-good-ways-to-strengthen-societal-innovation-in-the-united-states/.

[17] Villafranca, Omar, “Chip Shortage Cost U.S. Economy Billions in 2021,” *CBS News*, January 2022, https://www.cbsnews.com/news/chip-shortage-cost-us-economy-billions-in-2021/.

Finally, as the United States invests in these emerging technologies, it must also take a leadership role in setting standards for their responsible use. Due to their novelty, emerging technologies often become functional before legal and regulatory frameworks are established to govern them. The United States – together with its allies and partners – should be at the forefront of efforts to set norms for the use of disruptive technologies that reflect democratic values rather than allowing adversaries, namely China, to write the rulebook as it attempts to expand its techno-autocratic model.

Foster Private Sector Innovation

Figure 2. Federal and Business Shares of U.S. R&D Expenditures, 1956-2020



Source: CRS analysis of National Science Foundation, *National Patterns of R&D Resources: 2019–20 Data Update*, NSF 22-320, Table 6, February 22, 2022.

The private sector is the primary driver of technological innovation in the United States. As the figure at right shows, in 2020, U.S. businesses' share of research and development spending in the United States reached an all-time high of 73.1 percent, compared to the federal government's 19.5 percent.[18]

Recognizing that the private sector is vital to winning the U.S.-China technology competition, policymakers should establish a framework that provides financial incentives for technology companies in the United States to further invest in research and development in critical areas and ensures that global technology companies continue to view the United States as their investment location of choice. Such a framework must involve a combination of greater tax incentives for private research and development efforts, a removal of regulatory barriers to entry, and a policy approach that reflects the primacy of technological innovation to the health of the U.S. economy.

Fostering private sector-led innovation will also require growing America's technological workforce, including making substantial investments in science, technology, engineering, and math (STEM) education for the next generation of Americans. The Biden Administration should establish more programs for U.S. university students to work in both the public and private sectors in roles that impact national security. Washington should also establish more public-private partnerships in emerging technologies and other critical sectors, encouraging industry partners through tax or reputational incentives to allow their employees to temporarily serve as technical advisors to the U.S. government.

It is also imperative that policymakers reduce the number of hurdles for high-skilled foreign workers applying for a new or extended work visa in the United States. In 2018, U.S. Citizenship and Immigration Services (USCIS) adopted a much stricter policy approach to approving visa applications, expanding its ability to deny applications containing errors without first asking applicants to address them and expanding the range of cases under which it could remove foreign nationals. The policy

[18] Congressional Research Service, "U.S. Research and Development Funding and Performance: Fact Sheet," September 2022, https://sgp.fas.org/crs/misc/R44307.pdf.

disproportionately impacts workers in the fields of technology, science, and medicine, a net loss for the American people.[19] While any policy change should account for national security concerns, senior U.S. officials recognize that the vast majority do not immigrate with the intent of supporting intellectual property theft or forced technology transfers.[20] Instead, they have made substantial positive economic contributions to their host countries by creating jobs, building billion-dollar companies, and developing new technologies.[21]

The United States and its allies must ensure that their efforts to regulate technology and emerging technology industries do not impede U.S. companies' ability to innovate at scale. To this end, policymakers must give thoughtful consideration to the national security concerns raised by antitrust legislation and other bills targeting large U.S. tech companies. Anti-innovation legislative proposals target technology companies over their size without proper consideration of the unintended consequences of handicapping the science and technology enterprise that is key to U.S. national and economic security.

Some of the largest U.S. technology companies are some of the most substantial investors in emerging technology startups in the United States, a reality made possible by their size and revenue. In fact, for many startups, acquisition is the desired path forward, with some 58 percent of startup founders aiming to be acquired by a larger company rather than pursuing an initial public offering (IPO). [22] The business revenue losses resulting from some of the proposed antitrust legislation, aggressive antitrust enforcement efforts that target U.S. companies without respect for consumer harm, as well as the network usage fees being pursued by allies like the European Union (EU), Canada, and South Korea would cut directly into large companies' research and development efforts. Of course, the main beneficiary of a loss of U.S. investments in future research is the CCP, which subsidizes its technology giants in an attempt to leapfrog U.S. competitors.

Bolster Cloud Computing Security and U.S. Market Share

Securing the cloud is of critical importance to the United States and its ability to innovate. The cloud touches nearly every aspect of American life, powering databases, storage, email, and other artificial intelligence and large data applications central to our digital infrastructure. While this represents a large

[19] McCormick, Emily, "Foreign Tech Workers Face Higher Hurdles in Visa Applications," *Bloomberg*, July 2018, https://www.bloomberg.com/news/articles/2018-07-18/foreign-tech-workers-face-higher-hurdles-in-visa-applications?sref=5P9a6qw6.

[20] Zwetsloot, Remco, "US-China STEM Talent 'Decoupling:' Background, Policy, and Impact," Johns Hopkins Applied Physics Laboratory, 2020, https://www.jhuapl.edu/assessing-us-china-technology-connections/dist/407b0211ec49299608551326041488d4.pdf.

[21] ApplyBoard, "The Impact of International Students on Destination Economies in 2023," March 2023, https://www.linkedin.com/pulse/impact-international-students-destination-economies-2023-applyboard/.

[22] Goure, Daniel, "The New Arsenal of Democracy: The U.S. Commercial High-Tech Industry's Role in Countering the China Threat," *Lexington Institute*, June 2022, https://www.lexingtoninstitute.org/wp-content/uploads/2022/06/The-New-Arsenal-of-Democracy.pdf.

opportunity for economic growth, it also represents a vulnerability that requires policies that ensure our digital information is safe, reliable, and secure. While the United States is currently the global leader in cloud computing, Chinese companies are rapidly expanding in foreign markets and gaining traction in emerging markets, where most of the world's population growth is expected in the coming years. A global digital information ecosystem increasingly dominated by Chinese-manufactured cloud services would put the United States and its partners at risk. The Biden Administration must prioritize, invest, and advance efforts to secure the cloud and defend against threats to U.S. national security, while bolstering American cloud providers as they compete against China in foreign markets.

"A global digital information ecosystem increasingly dominated by Chinese-manufactured cloud services would put the United States and its partners at risk."

The past several years have seen cloud computing emerging as a new frontier in the race between the U.S. and the PRC to dominate the information supply chain. While leading domestic cloud providers – Amazon, Microsoft, and Google – often had the first-mover advantage, Chinese companies are expanding rapidly by leveraging state funding, leaning on PRC rules that favor domestic providers, and packaging cloud sales with investments in hard infrastructure and training. International regulations such as the European Union's Cybersecurity Certification Scheme for Cloud Services (EUCS) and South Korea's Cloud Security Assurance Program (CSAP) further impact the ability of U.S. companies to compete abroad.

The United States has a strong domestic cloud infrastructure, and the American market offers a diverse selection of cloud providers that support both domestic and international demand for cutting-edge cloud technology. Yet Chinese cloud companies supported by PRC initiatives, such as the Digital Silk Road are undercutting U.S. competitors on price to establish footholds in – and later dominate – emerging markets across Southeast Asia, Latin America, and Africa. Chinese companies are heavily subsidized by the state and can offer upwards of 40 percent cost savings compared to U.S. cloud computing services. In addition, foreign governments and businesses that sign contracts with Chinese cloud providers may find it difficult to switch providers down the road or face economic coercion if they try to do so.

While U.S. cloud computing companies lead globally, by some measures, Chinese cloud companies have already surpassed their American counterparts on barometers such as network scale. In Southeast Asia, for example, top Chinese cloud companies – Alibaba, Tencent, and Huawei – are each running more clusters of data centers, or "availability zones," than Amazon, Microsoft, or Google.[23] Chinese firms plan to invest hundreds of millions of dollars in developing markets across Southeast Asia in the coming years. As Chinese tech companies are increasingly pushed overseas by China's economic slowdown and

[23] Huang, Raffaele, "American Cloud Companies Face Challenge From China in Southeast Asia," *The Wall Street Journal*, February 2023, https://www.wsj.com/articles/amazon-microsoft-google-pressured-by-chinese-cloud-rivals-in-southeast-asia-2c8d98b4.

tightening regulations, Southeast Asia has become a priority market for PRC cloud providers, where they face less scrutiny and better chances of turning a profit than in more mature markets, such as North America and Europe.

"As Chinese firms continue to invest across developing nations, their customers will grow increasingly digitally dependent on Beijing, allowing the CCP to surveil and censor foreign populations and distort public opinion."

In recent years, the competition between the United States and the PRC in cloud manufacturing has been presented largely as a commercial challenge to American companies rather than a broader strategic and geopolitical threat to the United States. As Chinese firms continue to invest across developing nations, their customers will grow increasingly digitally dependent on Beijing, allowing the CCP to surveil and censor foreign populations and distort public opinion. While the PRC is selling customers in emerging markets a false sense of security through the allure of locally stored data, security is achieved through higher standards, not proximity.

The increasing aggression of Chinese competitors in cloud computing mandates a reassessment of the threat posed to U.S. national security and increased support from the Office of the U.S. Trade Representative for U.S. cloud companies. It also underscores the need to collaborate with allies and partners, strengthen norms of responsible state behavior, and hold countries accountable for irresponsible actions. U.S. and Chinese cloud services around the world are undergoing a strategic decoupling. As a result, countries that choose to partner with Chinese providers risk losing access to U.S. technological advancements. Cloud can also be used as a diplomatic gateway for the United States government to encourage countries in key regions to be more wary of the PRC's intentions and the risks such deals pose to information and technological security.

In addition to leveraging alliances to bolster Western cloud computing companies in their competition against Chinese companies, the United States must do more to secure cloud technology at home. In recent years, the U.S. has expanded its tools to prohibit or restrict certain information and communications technology and services (ICTS) transactions by foreign adversaries that are deemed to be an unacceptable risk to domestic national security. While the U.S. Department of Commerce has used more traditional tools, such as export controls to restrict companies namely China's tech giant Huawei in the telecoms arena, it must recognize that Huawei is the canary in the coal mine. The U.S. government should also use the ICTS supply chain authorities to secure cloud computing services in the United States.

In addition, policymakers should explore designating cloud computing as a critical infrastructure sector, which would increase the cybersecurity standards and resources available to U.S. cloud computing companies. For decades, a voluntary approach to cybersecurity for companies in the United States has made critical infrastructure vulnerable to cyberattacks from foreign actors, including the 2020 Russia-backed cyberattack against software company SolarWinds that compromised the data and networks of thousands of private companies and federal, state, and local government agencies. Equally important, policymakers should also develop comprehensive cybersecurity regulations for the nation’s critical infrastructure and improve cybersecurity across the government and private sector. While some efforts are already underway, the United States must accelerate these and other efforts to improve the security and resilience of the digital ecosystem.

Pillar Two: Strengthening Global Technology Alliances

The United States has a distinct advantage over its foreign adversaries: a deep, long-lasting network of allies and like-minded partners. As the United States seeks to contain digital authoritarianism and ensure its technological competitiveness, it must use these alliances to its advantage. Policymakers must prioritize working through multilateral forums to improve the resilience of the global technology supply chains that the United States relies on, including through onshoring, nearshoring, and friendshoring.

Washington should also leverage multilateral forums to secure data flows, both through agreements that incentivize strong data protections among our partners and by working with partners to regain our collective edge over global wireless telecommunications and maintain our lead in subsea cable networks.

Improve Supply Chain Resilience Through Nearshoring and Friendshoring

The COVID-19 pandemic laid bare how fragmented – and vulnerable – global technology supply chains have become, as evidenced by widespread shortages in products, such as semiconductor chips and the final goods that use them. At the same time, the pandemic exponentially increased our reliance on technology as people and businesses pivoted toward remote operations. These supply chain dependencies are vulnerable to exploitation. Indeed, in April 2020, President Xi Jinping gave a speech noting his intentions to control key supply chains, allowing China to cut off foreign countries during a crisis.[24]

As the United States seeks to avoid supply chain breakdowns during the next global disruption, policymakers must incentivize industry to make key dual-use products closer to home ("nearshoring") or in ally and partner countries ("friendshoring"). While the United States cannot competitively produce all technologies within its borders, it *can* ensure that critical technologies and their byproducts are designed, manufactured, and distributed in countries it can rely on, minimizing future disruptions.

> **"To avoid supply chain breakdowns during the next global disruption, policymakers must incentivize industry to make key dual-use products closer to home ('nearshoring') or in ally and partner countries ('friendshoring')."**

[24] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 2023, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/item/2363-2023-annual-threat-assessment-of-the-u-s-intelligence-community.

A second crucial benefit of creating such supply chain alliances is that they can help prevent strategic competitors from accessing certain advanced Western technologies, reducing the speed at which countries such as China develop technologies that may be used for harm. This is most effective when the United States and its partners take a coordinated approach to export controls and sanctions policies. The U.S. government can continue to implement targeted export controls and crack down on intellectual property theft; yet these actions will fall short if the countries with whom it does share its technology leave the door open for Beijing. The power of these technological coalitions is compounded when also used to shape standards for the responsible application of dual-use technologies.

One example of supply chain collaboration being used to bolster the national security of the United States and its allies can be found in the semiconductor industry. After the U.S. Department of Commerce implemented a series of export controls in October 2022 restricting China's ability to obtain certain advanced AI and semiconductor technologies with potential military applications, the Biden Administration brokered a deal with the Netherlands and Japan to restrict their exports of corresponding technologies to China,[25] compounding the impact of U.S. actions. Policymakers must continue to strike such partnerships with countries friendly to the United States to ensure advanced dual-use technologies do not fall into the hands of strategic competitors.

There are several existing alliances that policymakers ought to leverage to strengthen U.S. supply chains and contain the technological threats posed by China and Russia. The U.S.-EU Trade and Technology Council (TTC) was established in June 2021 to deepen cooperation on trade, technology, and security, including protecting and promoting critical technologies and infrastructure and collaborating on the development and deployment of new technologies based on shared democratic values. The council reflects a public desire for greater transatlantic technological collaboration: polling shows that the vast majority of voters on either side of the Atlantic believe the growing technological influence of China and Russia is a threat to their country's national security

One of the TTC's early successes was the coordination of Western sanctions against Russia in the wake of its brutal invasion of Ukraine. The group has since supported the coordination of Western controls on the export of dual-use technologies to Russia, as well as goods whose technological parts can be redirected toward Russia's war effort. The United States and the EU (European Union) should continue to work through the TTC to contain the threat of digital authoritarianism, including through existing working groups on secure supply chains, misuse of technology threatening security and human rights, investment screening, and export controls. Looking ahead, the TTC should also serve as a forum to raise concerns with the EU on its "digital sovereignty" agenda, including the Digital Markets Act (DMA), Digital Services Act (DSA), and other anti-innovation regulatory efforts that disproportionately impact U.S. technology companies' long-term ability to compete with Chinese competitors.

[25] Swanson, Ana, "Netherlands and Japan Said to Join U.S. in Curbing Chip Technology Sent to China," January 2023, https://www.nytimes.com/2023/01/28/business/economy/netherlands-japan-china-chips.html.

Other existing partnerships can help bolster the resilience of critical technology supply chains. Key partnerships and possible actions include:

- **The Indo-Pacific Economic Framework (IPEF):** Washington should continue to leverage IPEF – a group consisting of the United States and 13 Indo-Pacific countries – to deepen economic ties with partners in the region and counter China's digital footprint, including through the group's Supply Chains pillar. The IPEF countries should adopt procedural protections for all companies, similar to those adopted in the U.S.-Mexico-Canada trade agreement.
- **The U.S.-Japan-Republic of Korea Economic Security Dialogue:** Its inaugural meeting in November 2022 included a heavy focus on strengthening supply chain resilience, including in semiconductors, batteries, and critical minerals. In fact, Korea and Japan, along with Taiwan, are among the world's largest chip manufacturers, and some 23 percent of total U.S. semiconductor exports were destined for the Asia Pacific region in 2021.[26]
- **The Quad Dialogue:** Consisting of the United States, Australia, India, and Japan, this group continues to work together to secure technology supply chains, including a joint initiative to map capacity, identify vulnerabilities, and bolster supply-chain security for semiconductors and their components. India is a particularly important ally for the United States to cultivate, given its technological strength, market size, and deep talent pool of engineers, programmers, and STEM graduates.
- **The Americas Partnership for Economic Prosperity (APEP):** In its nascent stages of 12 countries in the Americas, APEP will focus on bolstering the region's competitiveness, including through more resilient supply chains.

In all efforts to nearshore and friendshore key technological supply chains, the United States must continue to act as a reliable trade partner in these areas regardless of political turnover, lest our partners opt out of the alliance.

Secure Data Flows and Encourage More Robust Data Practices Among Allies and Partners

We rely on the free flow of information for most aspects of modern life. Cross-border data flows underpin personal communications, commerce, and government relations. Yet without proper safeguards, malign state and state-backed actors can compromise sensitive U.S. data, breach user privacy, and engage in rampant intellectual property theft. To this end, the United States must leverage alliances to encourage strong cybersecurity and data protection practices at home and abroad, as well as counter China's expanding influence over data-sharing infrastructure that can be used for espionage.

[26] Semiconductor Industry Association, "SIA Applauds Launch of Indo-Pacific Economic Framework," May 2022, https://www.semiconductors.org/sia-applauds-launch-of-indo-pacific-economic-framework/.

Policymakers have made significant advances in bolstering cybersecurity and warding off data breaches within the United States (*see "Defending Against Digital Authoritarianism"*). Efforts such as the Biden Administration's National Strategy to Advance Privacy-Preserving Data Sharing and Analytics recognize that U.S. personal data is both a national security asset and a vulnerability if unsecured. More can be done, with many advocating for a comprehensive federal privacy law that sets minimum standards for what data can be collected and retained by companies operating in the United States. But while data security begins at home, it is not enough for the U.S. alone to model good behavior. To ensure that data shared with partners are not compromised, the United States must further encourage others to adopt strong privacy protections for data that flows into and is generated within their borders.

Just as the United States benefits from technology alliances to secure supply chains, it should use them to limit the transfer of sensitive data to trusted partners that share its values on digital freedoms. Where appropriate, Washington should strike multilateral and bilateral agreements that make the transfer of cross-border data conditional on the recipient jurisdiction having adequate levels of protections for user data, such as the upcoming U.S.-EU Data Privacy Framework.

"The United States must leverage alliances to encourage strong cybersecurity and data protection practices at home and abroad, as well as counter China's expanding influence over data-sharing infrastructure that can be used for espionage."

More broadly, Washington should continue to strike digital trade deals conditioned on strong data protections, such as the U.S.-Japan digital trade agreement. One opportunity to expand digital protections is through IPEF, where members such as Japan and Singapore are already pushing the group to finalize a so-called "digital-plus agreement" in 2023. As with past digital trade deals, policymakers should press for IPEF members to agree to comprehensive cross-border data transfer rules for the digital economy.

The United States can also incentivize the adoption of strong data privacy protections through normative means. In this respect, the Declaration for the Future of the Internet is a good first step in the right direction, with over 60 democracies and like-minded countries making commitments to respect data privacy laws and prioritize data protections.[27] As the United States continues to advance normative technological alliances, it should be careful not to exclude democratizing countries that are acting in good faith, lest this push them toward increased partnership with China.

A separate aspect of securing data flows is ensuring the infrastructure that allows us to share data in the first place. Subsea cables transmit up to 99 percent of international data, making them essential for the free flow of information. While the United States is a larger subsea cable provider than China, the CCP is providing state support to telecommunications companies to significantly expand their subsea cable

[27] The U.S. Department of State, "A Declaration for the Future of the Internet," April 2022, https://www.state.gov/declaration-for-the-future-of-the-internet.

operations in developing markets, often through predatory pricing. In addition, foreign adversaries can tap these underwater cables to collect data or even sever them to create internet blackouts.[28]

Meanwhile, the United States trails China in the global market for 5G and 5G-related services, with China's 5G base stations accounting for over 60 percent of the global total[29] and Huawei holding 30 percent of the 5G infrastructure market. No U.S. firms sell legacy 5G infrastructure abroad.[30] Foreign 5G networks raise national security concerns around the potential they serve as a means to conduct espionage and sabotage on the part of management companies, creating risks for U.S. persons and partners that rely on Chinese telecommunications companies. Despite U.S. officials warning allies and partners about the risks of allowing China to operate 5G networks, countries such as Germany, Brazil and Mexico continue to seek partnerships with Huawei for their 5G technology and infrastructure. What's more, the United States has fallen behind China in the race for 6G, threatening to increase this risk (*see "Protecting the Ability to Innovate*").

The United States must pool resources and work with its partners to regain their collective edge over global wireless telecommunications, maintain their lead in subsea cable networks, and counter illegal data breaches. Doing so begins with working through existing technology alliances and commercial partnerships, including the TTC.

[28] Khazan, Olga, "The Creepy, Long-Standing Practice of Undersea Cable Tapping," *The Atlantic*, July 2013, https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.
[29]Wilde, Crystal, "What's Really Going on With China and 6G?," https://www.6gworld.com/exclusives/whats-really-going-on-with-china-and-6g/.
[30] Allison, Graham and Eric Schmidt, "China's 5G Soars over America's," February 2022, https://www.wsj.com/articles/chinas-5g-america-streaming-speed-midband-investment-innovation-competition-act-semiconductor-biotech-ai-11645046867?st=hmjpsnr5e7nmxni&amp;reflink=article_copyURL_share.

Pillar Three: Defending Against Digital Authoritarianism

“Techno-autocracies,” such as China and Russia are increasingly using digital tools to limit internet freedoms, censor speech, spread disinformation and propaganda, and conduct surveillance both at home and abroad. Not only do these actions undermine democratic freedoms and electoral systems – they can also magnify the impact of kinetic attacks, as demonstrated by the Russian invasion of Ukraine.

As China, Russia, and like-minded nations seek to export their techno-autocratic model around the globe, it is imperative that the United States continue to level the playing field against anti-competitive market practices by strategic decoupling, heightening scrutiny of Chinese firms in the United States, and strengthening cybersecurity. Policymakers must also empower U.S. technology companies to continue acting as our first line of defense against state-backed cyberattacks against our nation and allies, including in the context of the Russia-Ukraine War.

Counter Chinese Digital Threats

Under the CCP, China has developed an internal model of digital authoritarianism, using AI, biometrics, and big data analytics to surveil its population and preemptively take action against citizens who are deemed a threat to its interests, including through racial and religious profiling. The CCP also relies on its extensive digital censorship apparatus to control the flow of data unfavorable to its interests, walling Chinese citizens off from the rest of the world through the “Great Firewall” and hiding the Chinese government’s malign actions, including its ongoing genocide against Uyghurs in the Xinjiang province and provocative actions in the South China Sea and Taiwan Strait. What’s more, the CCP’s capacity to exercise authoritarian governance is only expected to grow as the PRC continues to shape its legal system to strengthen the tools at its disposal.

Whether China succeeds in exporting this model of techno-autocracy across more of the world will hinge on its technological competition with the United States. Recent U.S. administrations have restructured foreign policy priorities to pivot military, economic, and diplomatic resources toward the Indo-Pacific in an effort to contain malign Chinese influence and access to advanced technologies. And there is bipartisan consensus in Congress about the threats posed by China, most recently reflected through generational investments in critical technologies through the CHIPS and Science Act of 2022 and the formation of the new U.S. House Select Committee on the Strategic Competition Between the United States and the CCP.

But more must be done. If it is to win its technological competition with China, the United States must double down on its investments in emerging technologies and the security of its cloud computing infrastructure (*see “Accelerating America’s Ability to Innovate”*) and leverage its unparalleled network of allies and partners to secure global technology supply chains and data flows (*see “Strengthening Global Technology Alliances”*). These are long-term propositions.

In the short-term, the United States must prioritize leveling the playing field with China. CCP-backed and -affiliated companies engage in rampant intellectual property and data theft, technology espionage, forced technology transfers for foreign businesses operating within China's borders, and malign influence operations in the United States. These practices not only undercut U.S. economic gains – they narrow the gap between U.S. and Chinese capabilities in critical and emerging technologies, weaken U.S. national security interests, and have a detrimental effect on U.S. firms.

Among Washington's most powerful approaches is technological decoupling from China. The Trump Administration raised the dangers of China's technology ambitions, and the Biden Administration has expanded the use of export controls on dual-use technologies flowing to Beijing to protect U.S. national security interests. Targeted technologies include semiconductor and other advanced computing technologies. The Biden Administration is also building out an outbound investment screening regime that places guardrails on U.S. investment in Chinese sectors of concern, including semiconductors, AI, and quantum technology. Washington should accelerate the process of decoupling from China on critical and sensitive technologies, while taking steps to avoid escalation. The U.S. Departments of Justice and Commerce, including the new Disruptive Technology Strike Force, will improve coordination on investigations and prosecutions of export control violations, which is a step in the right direction.

Policymakers should also heighten scrutiny over Chinese companies that seek to or are operating in the United States to prevent data and intellectual property theft, technology surveillance, and malign influence operations. Policymakers should implement President Biden's June 2021 Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries by creating robust national security risk frameworks used to evaluate apps owned or controlled by foreign adversaries. Policymakers should also expand the resources available to the Committee on Foreign Investment in the United States (CFIUS) as it assesses the risks posed by PRC-backed entities seeking to acquire U.S. technology. Where unfair or aggressive practices are discovered, Washington must make clear to Beijing that these activities carry consequences and enlist its allies in this effort for an even greater impact.

In all instances, the Administration and Congress must work together to use every legal recourse to hold China accountable for its unfair market practices and technology theft, including through unilateral measures when necessary.

Counter Russian Digital Aggression

In the aftermath of Russia's brutal invasion of Ukraine, Russian President Vladimir Putin continues to wage constant cyberattacks against Ukraine and its allies to disconnect them from the internet, bring down critical infrastructure, and spread dangerous disinformation to build support for Russia's assault on democracy, all while censoring its own citizens. Between 2020 and 2022, Russia increased its targeting of users in Ukraine by 250 percent, while the targeting of users in the North Atlantic Treaty

Organization (NATO) countries increased by 300 percent.[31] In Ukraine, attacks largely focused on its government and military entities, critical infrastructure, utilities, and media. Alarmingly, some of these cyberattacks have been launched in tandem with missile and ground attacks, highlighting the destructive power of Russia's hybrid warfare.

Throughout the conflict, U.S. technology companies have proven they are the West's best defense in countering Russian cyberattacks and disinformation campaigns, minimizing disruptions to the Ukrainian people, and exposing Russia's brutal actions for the world to see. American companies have played a vital role in the conflict, working with Ukrainian organizations to share real-time threat assessments and protecting critical infrastructure. Many maintain open channels with U.S., EU, and NATO officials, sharing intelligence vital for assessing cyber threats and vulnerabilities.

Meanwhile, firms such as Amazon, Apple, Google, and Microsoft are investing billions in bolstering cybersecurity, while social media platforms, such as Meta and Twitter, are deleting dangerous disinformation sewn by the Kremlin. Google temporarily disables Maps' live data location features within Ukraine to deny Russia insights into the locations of Ukrainian forces. SpaceX has also been instrumental in its ongoing efforts to use rapid patching to overcome Russian cyberattacks on satellites, thereby allowing the Starlink satellite network to provide virtually uninterrupted internet service to Ukraine despite damage to on-the-ground infrastructure.

U.S. technology companies are on the digital front lines of Russia's war with Ukraine. As Russian cyberattacks against Ukraine and its allies increase in frequency and destructiveness, the U.S. government should be strengthening, not weakening, the domestic technology industry.

Moscow poses serious digital threats beyond its war with Ukraine. According to the U.S. intelligence community, Russia is expected to remain a top cyber threat as it refines its espionage, influence, and cyberattack capabilities, with a particular focus on improving its ability to target critical infrastructure in the United States and allied and partner countries.[32]

The Kremlin and Putin-backed actors will continue to spread disinformation and propaganda through official Kremlin or ministry statements, state-funded foreign- and domestic-facing media, Russia-aligned outlets with global reach, local-language specific outlets, bots, and false social media personas.[33] These disinformation campaigns have historically been used to undermine faith in democratic entities such as NATO, the EU, national governments, and – of particular concern – electoral institutions. The Kremlin also views disinformation campaigns as a tool to sow discord between communities and stoke civil unrest. Ahead of the 2020 U.S. presidential election, for example, documents leaked showing that a

[31] Google, "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape," February 2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

[32] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community."

[33] U.S. Department of State, "GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem," August 2020, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

Kremlin-linked oligarch intended to exacerbate racial divisions to “destabilize the international situation in the U.S.”[34]

In response to these ongoing threats, policymakers must continue to strengthen cybersecurity in the public and private sectors, including through increased resources and authorities for the Cybersecurity and Infrastructure Security Agency. The Biden Administration is moving federal agencies to a zero-trust architecture and directing agencies to implement post-quantum cryptography, a step in the right direction. Emphasis must be placed on bolstering electoral cybersecurity, particularly ahead of key election cycles. Policymakers should also consider growing the U.S. Department of State’s Global Engagement Center, which coordinates efforts to recognize, understand, expose, and counter foreign propaganda and disinformation.

In addition, legislative and executive actions that would hamper critical technology actors should be subject to an interagency national security review to ensure they don’t have unintended consequences for partners starting with allied operations in Ukraine, as well as for other hybrid wars on the horizon.

Finally, the U.S. government must also bolster cooperation with social media platforms where disinformation and propaganda can thrive. Such partnerships might focus on doubling down on awareness efforts about Russian propaganda sources and their nature, as well as digital literacy initiatives that better prepare citizens to identify and avoid cyber-aggressions.

“Legislative and executive actions that would hamper critical technology actors should be subject to an interagency national security review to ensure they don’t have unintended consequences.”

Conclusion

As Washington goes head-to-head with Beijing in the race for technological superiority, the United States and its partners must urgently realign its policies and regulations to advance domestic technological competitiveness. This will require aggressively supporting our own technology sector by investing in the emerging technologies that are foundational to the 21st Century, creating incentives for technology companies to further invest in research and development in the United States, and bolstering cloud computing cybersecurity to protect our digital infrastructure from foreign adversaries. At the same time, Washington must avoid any legislation that has the potential to hamstring U.S. innovation potential.

To maximize the impact of its domestic investments and secure cross-border data flows, the United States should use its deep network of alliances to improve the resilience of the global technology supply

[34] Engel, Richard, Kate Benyon-Tinker, and Kennett Werner, “Russian Documents Reveal Desire to Sow Racial Discord – and Violence – in the U.S.” *NBC News*, May 2019, https://www.nbcnews.com/news/world/russian-documents-reveal-desire-sow-racial-discord-violence-u-s-n1008051.

chains that we rely on and leverage multilateral forums to secure data flows. And policymakers must make every effort to level the playing field against China and Russia, practicing strategic decoupling, heightening scrutiny of Chinese firms in the United States, strengthening cybersecurity, and empowering U.S. technology companies to continue acting as our first line of defense against state-backed cyberattacks.

The technological competition between the United States and China will determine the future of the free world. The choices the United States makes today will shape the strength of our national security, the prosperity of our economy, and the health of our democracy for decades to come. There is no time to lose.

> **"The technological competition between the United States and China will determine the future of the free world."**

Acknowledgments

This national security policy framework was published by the American Edge Project along with the following contributors:

- **General Joseph Dunford**, former Chairman of the Joint Chiefs of Staff and American Edge Project National Security Advisory Board Co-Chair
- **Michael Morell**, former Acting Director of the Central Intelligence Agency and American Edge Project National Security Advisory Board Co-Chair
- **Frances Townsend**, former White House Counterterrorism and Homeland Security Advisor and American Edge Project National Security Advisory Board Co-Chair

###