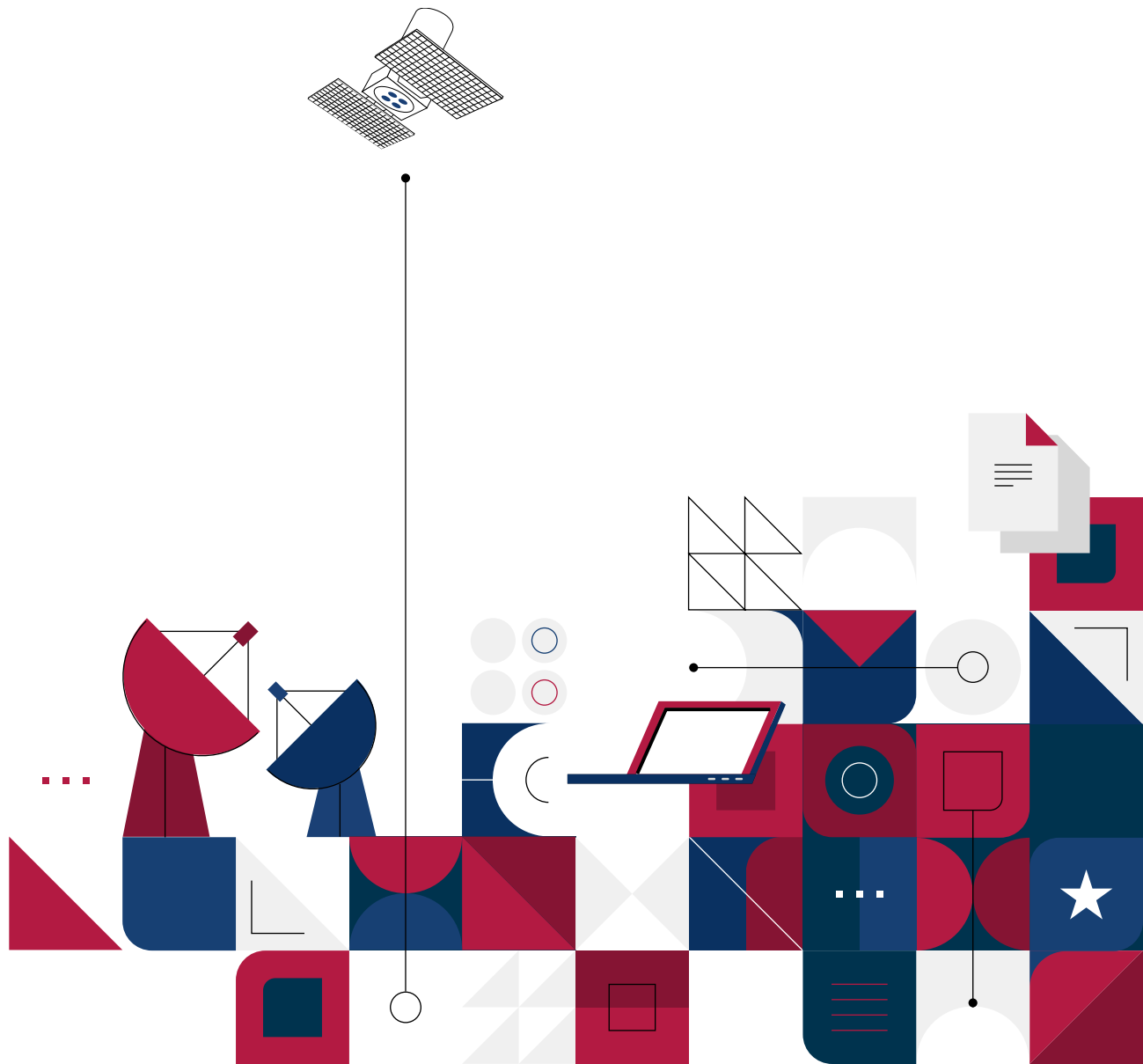




SPECIAL COMPETITIVE
STUDIES PROJECT

Mid-Decade Challenges to National Competitiveness

September 2022



Board of Advisors

Dr. Eric Schmidt, Chair

Dr. Nadia Schadlow

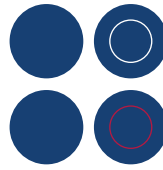
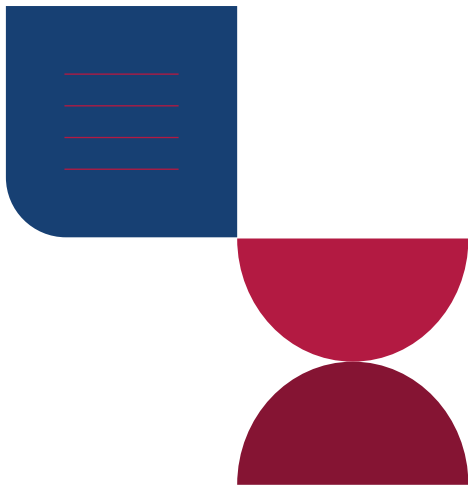
Robert O. Work

William “Mac” Thornberry III

Michèle Flournoy

The SCSP Board has provided intellectual leadership since the project’s inception. Each Board member embodies patriotic national service in their accomplished careers that they have carried into the Project. Their combined vision forms the conceptual foundation for strengthening our national competitiveness: Nadia Schadlow’s foresight about the future of national security strategy, Bob Work’s deep thinking on the changes to conflict wrought by technology, Mac Thornberry’s commitment to always connect big national security ideas to the interests of the American people, Michèle Flournoy’s keen focus on the practical defense challenges facing the United States, and Eric Schmidt’s steadfast determination to help the United States recognize the stakes of technology competition and help the nation organize to win.

Ylli Bajraktari, CEO



From October 2021 until August 2022, SCSP organized 4 board meetings and 26 panel meetings with more than 225 experts, including government officials, technologists, academic leaders, and many others. The SCSP staff also conducted more than 400 engagements with leaders from the private sector, academia, civil society, and government. We are grateful for the time and effort of those we have consulted. This report is the culmination of the SCSP staff's work up to this point in its mandate and its effort to synthesize the wealth of information gathered from all of the individuals and entities with whom we have engaged. Although not everyone we have engaged with may endorse this report, we hope it reflects the key points we have learned and charts a path for action.

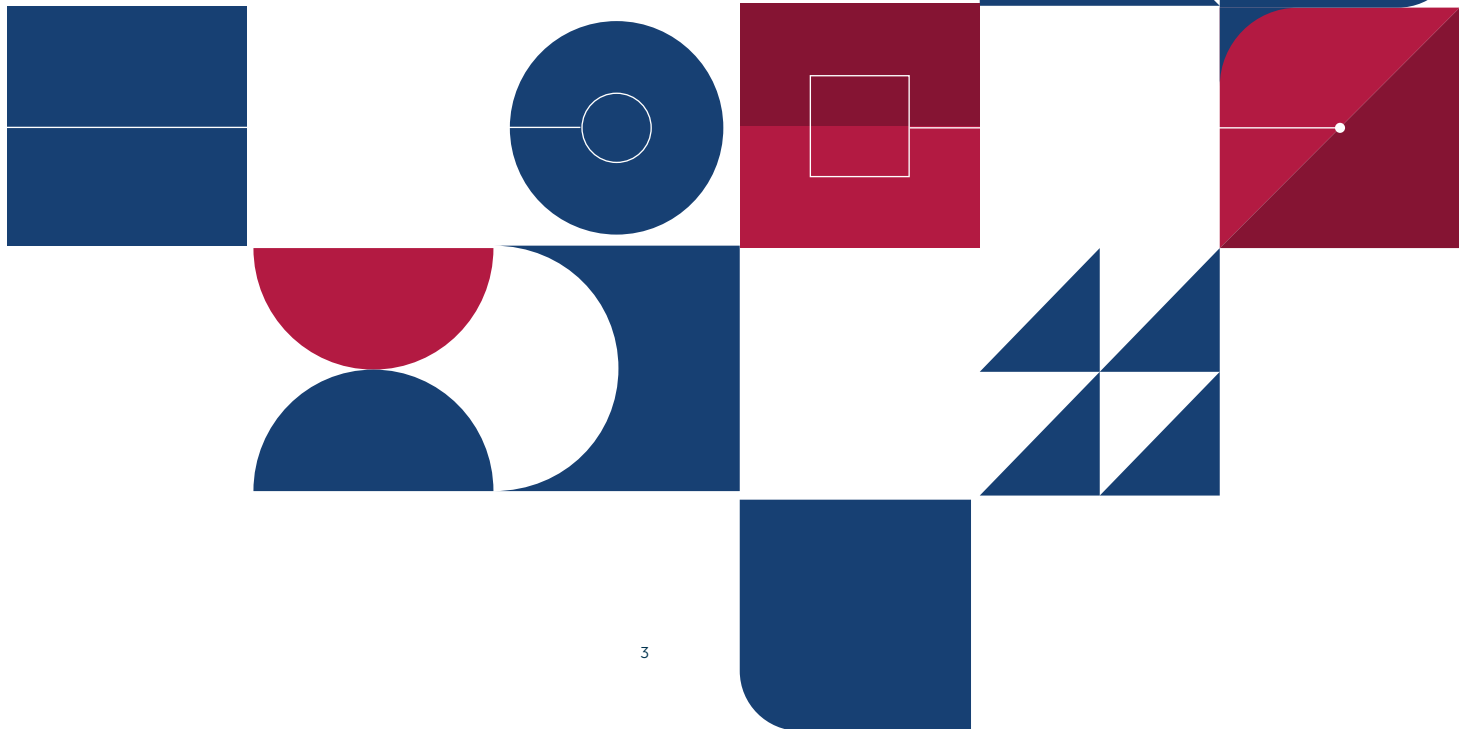


Table of Contents

i

A Letter from

Dr. Henry A. Kissinger

ii

Preface

Why SCSP

iii

Introduction

A Contested Future

iv

A Competitiveness Agenda

The Six Challenges
the United States
Must Win

1

Chapter 1

Harnessing the
New Geometry of
Innovation

2

Chapter 2

Restoring the Sources
of Techno-Economic
Advantage

3

Chapter 3

An American
Approach to AI
Governance

4

Chapter 4

Remaking U.S. Global
Leadership in the
Age of Technology
Competition

5

Chapter 5

The Future of
Conflict and the New
Requirements of
Defense

6

Chapter 6

Intelligence in an
Age of Data-Driven
Competition

7

Chapter 7

The Technologies
That Will Drive
Future American
Competitiveness

a

Appendix

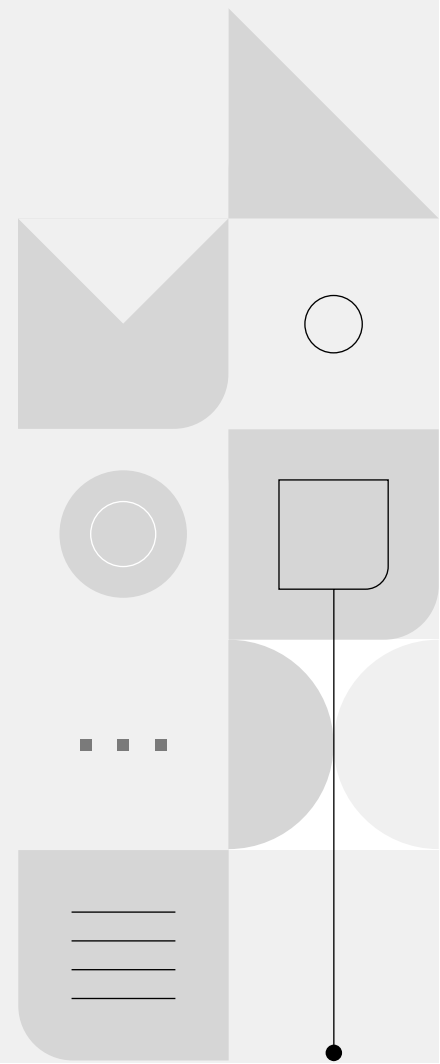
Contribution List

A LETTER FROM

Dr. Henry A. Kissinger

In the 1950s, Nelson Rockefeller created the Special Studies Project – a bipartisan effort to define the major problems and opportunities that the United States confronted as it shifted from the aftermath of World War II and faced an ideological competitor striving for nuclear parity. I was asked to serve as the Executive Director. We brought together some of the leading thinkers of our country and produced a series of papers that became the book *Prospect for America*, which we hoped would explain the issues facing our country that may have been hard for the government to tell the American people. We wanted to help Americans understand these challenges, build consensus around ways to navigate them, and ensure our democratic way of life prospered.

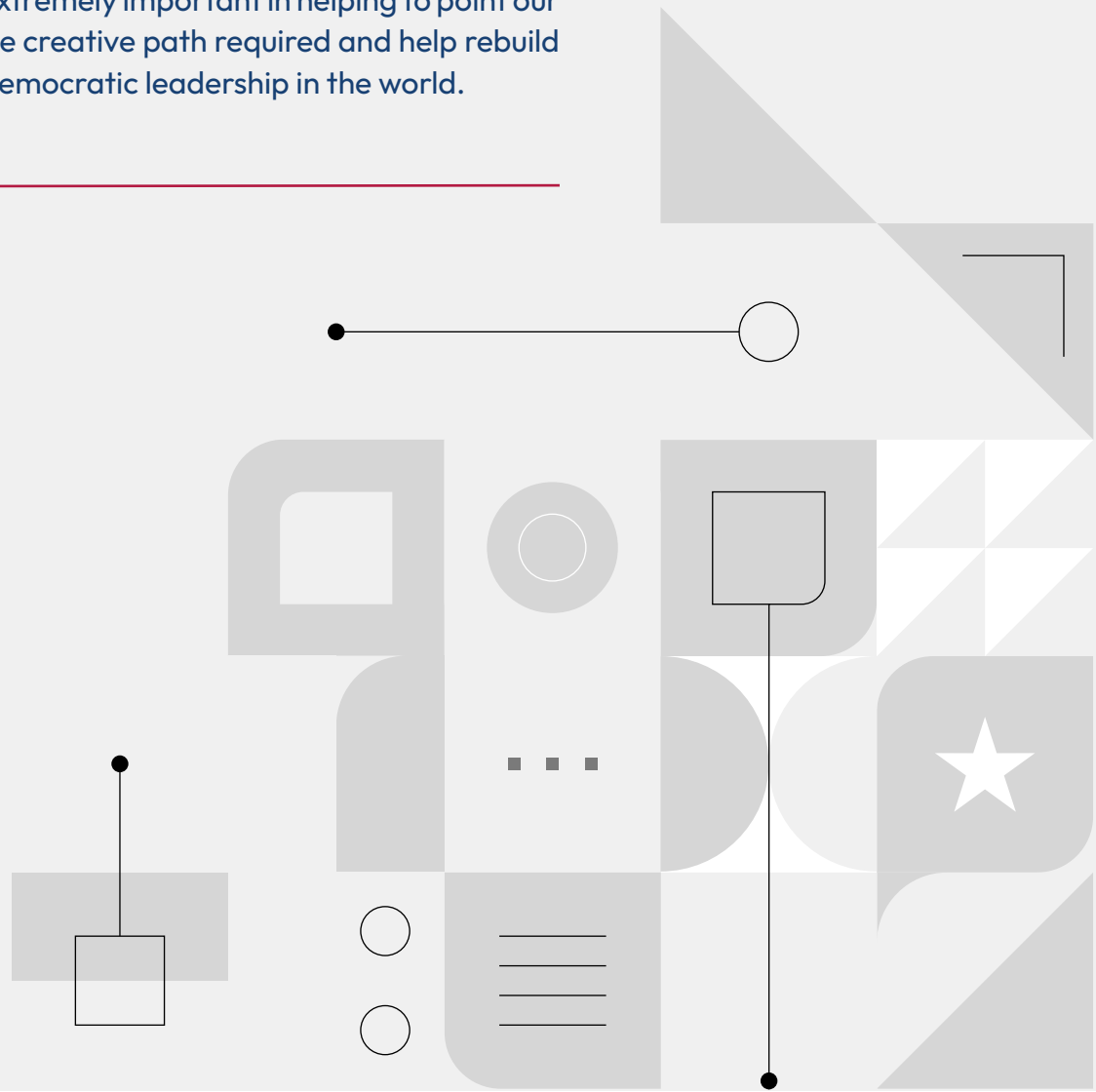
Two developments that are shaping the international security environment today mirror the situation in which the Special Studies Project conducted its work. First, there is an intensifying competition for strategic advantage between the United States and China, and, second, advances in artificial intelligence and other emerging technologies promise to bring tremendous impacts on both economic and military competitiveness, as well as our society. There is also a sense among democratic countries that we are losing confidence in our system of government. Our country needs a discussion of the changes that are taking place, the



challenges to come, and to define the direction and purpose for our country in this new strategic environment.

This is why I congratulate Eric for launching this new effort and why I am happy that so many great minds are participating. For this project, you need broad participation from the public and private sectors, as well as dialogues with our Allies, about the future of the international security environment shaped by these technologies. There may be huge differences in opinions on how to handle the issues before us, but our government and society must find a unifying purpose and face these challenges with the same imagination, decisive action, and national will we have summoned at other critical junctures in our history.

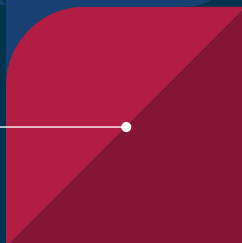
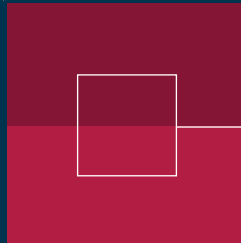
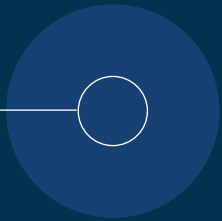
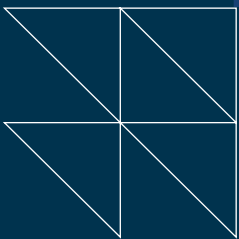
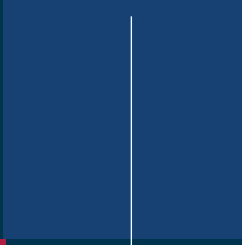
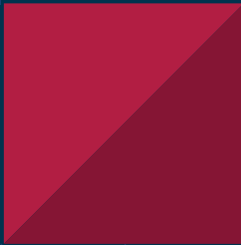
Thank you all for doing this, and Eric and Ylli for leading it. This effort can be extremely important in helping to point our country towards the creative path required and help rebuild confidence in our democratic leadership in the world.



Why SCSP

Mid-Decade Challenges to National Competitiveness





PREFACE

Why SCSP

Today Americans need a new unity of purpose. Three decades of American beliefs about themselves, their government, and their place in the world have been shaken. In the midst of a wave of technological change, we are left with questions about the future of democracy, rising geopolitical danger, and disorientation about where we are heading.

We created the Special Competitive Studies Project (SCSP) to develop an agenda that can help Americans recapture the confidence to face these challenges with a shared sense of national purpose. SCSP's mission is to make recommendations to strengthen America's long-term competitiveness for a future where artificial intelligence (AI) and other emerging technologies reshape our national security, economy, and society.

The premise of our work is straightforward. Strategic competition between the United States and the People's Republic of China (PRC) is the defining feature of world politics today. The epicenter of the competition is the quest for leadership and dominant market share in a constellation of emerging technologies that will underpin a thriving society, growing economy, and sharper instruments of power. At stake is the future of free societies, open markets, democratic government, and a world order rooted in freedom not coercion.

Why Competitive? Competition is SCSP's organizing principle. It frames the three major dynamics shaping our world — geopolitical rivalry, technological promise, and the ideological contest between democracy and autocracy.

- *Geopolitical Rivalry.* Competition with China imposes a new lens on most significant trends impacting the United States and the world. The PRC is the United States' chief ideological opponent, largest economic competitor, technology peer, most capable military challenger, and most powerful geopolitical rival for the foreseeable future. China is creating spheres of influence without any clear limits, underpinned

by physical and technological infrastructure, cemented with commercial ties and technology platform dependence, deepened by authoritarian affinities, and enforced by growing military capabilities. Its goals are to exercise control in the Indo-Pacific, extend its influence globally, and ultimately remake the international order.

- *Technological Promise.* A constellation of emerging technologies is ushering in an era technologists call an “exponential age”¹ and the beginning of “the most important century of all time for humanity.”² Foundational technologies – often powered by AI – are producing new discoveries and applications that will improve quality of life and solve some of the hardest scientific challenges. Today’s tech wave, driven by digital technologies, is now cresting. The next tech wave, building on digital breakthroughs, is in the physical and biotechnical domains. The states and companies that harness this wave of “ABC” foundational technologies – atoms, bits, and cells – will win the future. China is intent on supplanting the United States as the world’s innovation hub. Without such a competitor, many of the technological developments underway could be seen as areas for collaboration or merely of commercial interest. Instead, the technology competition has become a key element of a systemic competition over world order.
- *Democracies Tested.* The post-Cold War democratic ascent is over. Democracies are disoriented and in search of equilibrium in a technology-enabled society. Citizens want to protect their rights and their freedoms, and still enjoy the benefits of digital connectivity. Tech-skepticism threatens to stall innovation and adoption. Governments are attempting to moderate online content, fight disinformation, and protect privacy while unlocking the benefits of data, and also confronting the consolidating power of large companies without stifling innovation, over-extending government power, or sacrificing core liberties. It is a tall agenda. As democracies pursue different paths to tech governance, they risk dividing the community of democracies. Meanwhile, autocracies are seemingly ascendant. They are harnessing technology to deliver the benefits of modernity and extend government control. Beijing’s brand of autocracy recasts the challenges within democracy as part of a larger referendum for how best to organize modern society.

1 Azeem Azhar, [The Exponential Age: How Accelerating Technology is Transforming Business, Politics and Society](#), Diversion Books (2021).

2 Holden Karnofsky, [The Most Important Century \(in a nutshell\)](#), Cold Takes (2021).

These three futures must be tackled together in a comprehensive competitive agenda. The geopolitical rivalry is intimately connected to harnessing the technology wave. The stakes of the technology waves become sharper when viewed through the lens of rivalry. The nature of different political systems will determine how technologies are developed and used, and the success of democracies and autocracies in using technologies will help to determine the broader appeal of each governing system in a long-term competition. There will be winners and losers.

From NSCAI to SCSP. Intellectually and organizationally, SCSP grew from the Congressionally-mandated National Security Commission on Artificial Intelligence (NSCAI). SCSP's leadership and some of its staff worked on that project. NSCAI accomplished a great deal as an independent commission established under one presidential administration and concluding under a second. It succeeded foremost in informing the U.S. Government — Congress and the Executive Branch — and the American people about the multifaceted implications of AI and associated technologies for national security. It identified technology as the central element of the rivalry between the United States and China, explained why the United States must organize to compete, and provided blueprints for action. We knew, however, that NSCAI left much unfinished business. Getting AI right was only the beginning. The commission quickly realized a constellation of technologies could lay claim to broad strategic import across economic and national security applications. Winning a technology competition requires comprehensive focus across the full range of them. SCSP will expand the “tech list” and develop blueprints for action. Our new project is privately funded, but it remains publicly minded and staunchly nonpartisan in believing technology, rivalry, competition, and organization remain enduring themes for national focus.

Model from the Past. We found a nearly perfect model for the level of ambition befitting our challenges in a 1950s era Cold War study led by Henry Kissinger called the Rockefeller Special Studies Project. It marshaled expertise from across American society to bring coherence and direction to a national agenda at the beginning of a new era. The group — drawn from industry, academia, and government — believed America needed a forward-looking response to the era's many upheavals. Their message resonated with SCSP. “A nation which does not shape events through its own sense of purpose,” they wrote, “eventually will be engulfed in events shaped by others.” They appreciated the close correlations between foreign and domestic policies and the importance of science and technology leadership to wider trends. They kept at the fore a positive outlook that defined strategic competition as a “struggle *for* something.” The project provided clarity about America's ideals, honesty about its shortcomings, and ideas for improvements at home that would help persuade friends abroad.

Non-Partisan Agenda. SCSP sees the core challenges facing America as non-partisan in origin and solution. SCSP's goal is to provide a roadmap for strengthening America's competitiveness, armored against changes in political sentiment or leadership and recognizing the central role played by a wave of technologies changing our world. SCSP will not have all the answers. Our first step is to bring together a diverse group of Americans to frame the challenges, outline an agenda, and provide actionable recommendations for the United States to lead in the technology competition. There is a path to a safer, healthier, free, united, and more competitive nation.

The SCSP Process. Inspired by this example, SCSP draws contributors from across American society united in the mission to strengthen U.S. competitiveness. We also intend to extend our work to bring in foreign counterparts and organizations who share our outlook on the global nature of this competition. The project seeks to clarify the nature of the strategic challenge the United States and its partners face and anticipate how it may evolve. And it will help to build what the original SSP project members called a "working consensus" that allows a vast and diverse democracy to "get ahead with its business." SCSP is divided into six panels on technology platforms, economy, society, foreign policy, defense, and intelligence. Each is pursuing solutions to its respective mid-decade challenge, works with its own advisors and objectives, and will publish its own detailed reports over the life of the project.

The Report. This report sets an agenda for a strategy of technology-centered national competitiveness. The report is an initial *why* and *what* that outlines the logic for action and an agenda for the future. Where immediate opportunities exist, the report highlights areas for federal action. However, it is far from the sum-total of the project's work or a comprehensive set of recommendations.

Next Steps. The remainder of the project will be focused on the *how* of the competitiveness agenda. SCSP's ambition is to develop detailed action plans for technology priorities, organizational requirements, resource recommendations, and to bring the private sector, government, academia, and civil society, and U.S. allies and partners together for a common purpose. These action plans will follow in the coming year.

The Need for National Purpose. While the SCSP agenda is focused on technology and national security, the project's motivation is deeper. Americans and the democratic world have experienced a difficult few years –the wider impact of emerging technologies on our lives, a once in a century pandemic, Russia's invasion of Ukraine, and our own society's polarization. Disillusionment is a real concern. And pessimism threatens to paralyze action. We see the opportunity to rebuild a mission around an enduring national purpose.

America's purpose is anchored in protecting the rights of the individual within a democratic system. The United States stands for human dignity, universal rights, and the principle that governments serve the people. America represents an experiment in human liberty, not its culmination. It is an example of a society that can recognize its faults and can also correct them. The U.S. Government's role in supporting the purpose is outlined in the U.S. Constitution: "to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity."

America's purpose is also the foundation of its strength even if we do not always live up to the ideal. Enduring purpose can orient our actions. Americans want to look to the future. They want to innovate, and they want to demonstrate the superiority of a society where free people live under a democratic government. We should not lose sight of our advantages, dwell on our weaknesses, or lower our ambitions. If we do, we hurt the prospects for democracy in the world and create our own obstacles to action.

There is a long history of misguided anxiety in American life about whether a free and unruly pluralistic society such as ours can compete with the central planning and seemingly forceful dictates of authoritarian regimes. The members of the 1950s Special Studies Project had more confidence: "the power which is generated by the voluntary effort of a free people cannot be equalled by the reluctant compliance of subject nations." An equally good lesson for today's competition.

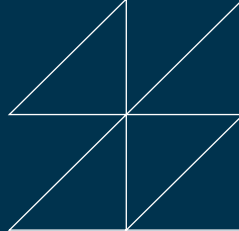
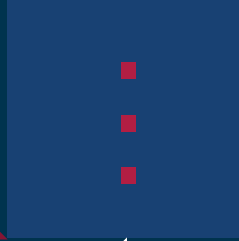
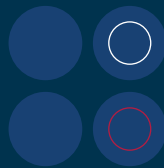
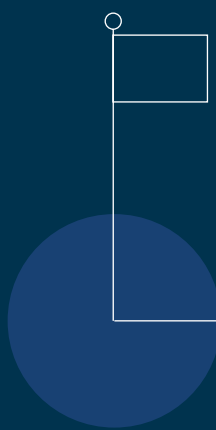

Eric Schmidt


Ylli Bajraktari

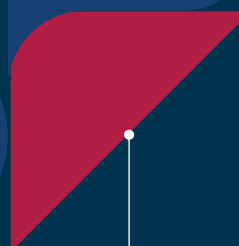
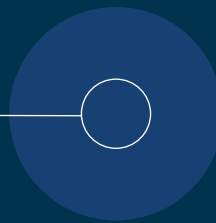
A Contested Future

Mid-Decade Challenges to National Competitiveness





- What Does Losing Look Like?
- How We Got Here: A Story of Strategic Surprise
- The Geometry of Innovation Has Changed
- Tech Trendlines are Concerning
- Three Futures
- Why 2025-2030
- Remembering American Advantages



INTRODUCTION

A Contested Future

A contest for the future is unfolding. By the end of this decade, we will know if we will live in a world shaped by free expression, tolerance, and self-determination or dictated by censorship and coercion. We will know whether a government for the people or a government that dictates to the people prevails in the contest to organize modern societies. We will know whether a wave of technological innovation is applied to improve society and human welfare or directed for control and conquest. How this future plays out will be shaped by the technology competition between the United States and China.

What Does Losing Look Like? What would it look like if the overall technology competition went the wrong way? Understanding the stakes requires imagining a world in which an authoritarian state controls the digital infrastructure, enjoys the dominant position in the world's technology platforms, controls the means of production for critical technologies, and harnesses a new wave of general purpose technologies like biotech and new energy technologies to transform its society, economy, and military.¹ In that future:

- *China dominates the economy of the future and captures the trillions of dollars' worth of value generated by the next wave of technologies.* The United States and its allies lose out on the majority of the jobs and growth promised by the new technologies. Supply chains for the new technologies are built in China. China controls the design and production of solar, wind, and nuclear energy technology and uses its chokehold over other nations' climate transitions as leverage. Its dominance of tech sectors creates powerful platforms and companies that replace U.S.-based companies in key areas including cloud services, social media, and Internet search.
- *China's tech sphere of influence spans the globe.* China uses its techno-economic advantage for political leverage. Nations - including U.S. allies - reliant on China's tech swing into the PRC's political orbit. Countries dependent on China's digital

¹ See Chapter 7 of this report for further discussion of general purpose technologies.

infrastructure and platforms (atop existing hard infrastructure and commercial dependencies) are unwilling to risk crossing Beijing in a global crisis. They support the PRC's political ambitions in multilateral venues. And they accommodate its voracious demand for data of all kinds that flow through the networks for the PRC's security and economic ambitions.

- *Authoritarian regimes sell the case that they are masters of the modern world.* China and Russia make their profession of “no limits” friendship a reality, locking in an authoritarian ascent. Countries begin to emulate the authoritarian governing model, technology-enabled surveillance and social control, and an elevation of the needs of the state over the fate of individuals and the rule of law. They rally around a vision of order espoused by Beijing and Moscow.
- *An open internet is compromised, and frictionless digital oppression replaces digital freedom.* The PRC's vision of a “sovereign” internet sweeps the globe atop infrastructure built by platform companies based in China. China's surveillance state is globalized. PRC-backed platforms replace other global platforms and shape the global discourse using inscrutable algorithms to tailor messages to undermine democracies and support PRC political objectives. The PRC exercises control of the digital payment infrastructure. It collects vast amounts of data that can be applied to target individuals and refine its propaganda. Democracies abandon a global Internet and retreat into their own splinternets to protect their security and digital public squares, but even this is a losing endeavor as TikTok and other PRC-based platforms dominate global markets.
- *Nations' digital infrastructure is cyber-compromised.* The world will be dependent on China for most core digital technologies, key electronics components, and finished products woven into every critical system. Energy grids, ports, airports, financial systems, and government offices will be vulnerable to PRC cyber exploits. Beijing uses them as threats during a disagreement and deploys them as cyberattacks in a crisis.
- *The U.S. military's technological edge erodes.* The PRC annexes Taiwan. U.S. defense commitments and power projection are threatened. China uses its dominant position in autonomous systems, robotics, and low-cost mass manufacturing, augmented by PRC control of global networks, to build weapons systems that overmatch U.S. capabilities, create new warfighting paradigms, and erode confidence in the U.S. military deterrent. The combination of reduced capability and allies hedging forces the United States to sacrifice its positions on

Taiwan.

- *The PRC cuts off the supply of microelectronics and other critical technology inputs.* Beijing makes good on its threats to cut off the U.S. supply of rare earth minerals – necessary for energy, digital, and defense technologies – and cuts off the supply of leading-edge semiconductors, 92 percent of which are produced in Taiwan.² America’s military is crippled, and the nation is plunged into a depression. Americans are forced to live in a world where China can turn off the technology tap.

In total, this picture amounts to the unraveling of the order the United States and the democratic world built after World War II and a serious challenge to future U.S. prosperity. The United States and other democracies would become economically dependent, losing their engines of prosperity and freedom of action in the world. Leaders would face hard choices. They would have to compromise beliefs, sacrifice allies to secure a place in a different world order, or fight to sustain the U.S. position from a smaller techno-industrial base, worse geopolitical position, and diminished military advantage.

Even if only some of this came to pass, the world would be a darker place for the United States and democracy. Losing the competition with China is not just about preserving abstract principles and political institutions – it will lead to the transformation of our daily lives in ways that will be impossible to ignore. Already, we have seen how China wields its platform advantages to extract data, coerce compliance, and punish individuals, companies, and nations that do not act in accordance with its wishes or criticize PRC policies.

A losing scenario is plausible. If we consider the state of the technology competition – how we got here, how prepared we are to harness emerging technologies today, and where trendlines suggest we are going – there is ample reason for concern.

How We Got Here: A Story of Strategic Surprise in Three Battlegrounds. Three technology battlegrounds today – microelectronics, fifth-generation wireless technology (5G), and AI – tell the story of a nation (and its allies) coming perilously and unwittingly close to ceding the strategic technology landscape and along with it the capacity to shape the future. These three technologies represent the critical hardware, network infrastructure, and software underpinning every aspect of our lives – the computing power, connectivity, and data flows critical to our economy, society, and national security. Only determined efforts by two U.S. administrations, and by Congress in just the last few years, averted

² Antonio Varas, et al., [Strengthening the Global Semiconductor Value Chain in an Uncertain Era](#), Boston Consulting Group and Semiconductor Industry Association at 5 (2021).

crises that were decades in the making. But the larger story is one of reactive policymaking, positional weaknesses, a disconnect between private sector technological strength and national requirements, being out-organized by a determined rival, and more fundamentally a failure to connect technology developments to strategic competition.

- In microelectronics, the United States stood by as its share of manufacturing for the chips that power every modern machine reached a historic low, with all high-end chip manufacturing done by a few companies located in East Asia.³ 98 percent of the chips the Pentagon needs are now built, assembled, or packaged in the PRC's shadow.⁴ Congress and the White House stepped in via the CHIPS and Science Act, which includes an emergency infusion of billions of dollars to rebuild manufacturing capacity and drive new leading-edge research at home. But even with swift implementation, regaining manufacturing leadership, addressing the workforce problems, and ensuring supply chain resiliency will require more policy actions and deeper public-private coordination.
- In 5G, PRC-backed companies were on their way to controlling network hardware for swaths of the global Internet. The United States had no market-ready alternative. Only a U.S. diplomatic campaign warning of the risk of dependence on the PRC and U.S. export controls on select microelectronics slowed China's 5G march. Yet the race is just beginning to develop 5G applications in autonomy, advanced manufacturing, and Internet of Things (IoT).
- AI could represent the next chapter of the industrial revolution. Intelligent systems and applications driven by computing power, algorithms, and data will connect a constellation of technologies to transform entire industries. In 2017, 280 million people in China – close to the entire U.S. population – witnessed AlphaGo defeat

Three technology battlegrounds today – **microelectronics, fifth-generation wireless technology (5G), and AI** – tell the story of a nation (and its allies) coming perilously and unwittingly close to ceding the strategic technology landscape and along with it the capacity to shape the future.

³ [2021 State of the U.S. Semiconductor Industry](#), Semiconductor Industry Association at 10-19 (2021).

⁴ [Deputy Secretary of Defense Dr. Kathleen Hicks' Remarks at the White House CHIPS-Plus Act Event](#), U.S. Department of Defense (2022).

their Go champion 3-0.⁵ China organized for victory. While the United States had no AI strategy linking the tech to national security, China started investing in a national plan to lead the world in AI by 2030. In the United States, a federal commission, the National Security Commission on Artificial Intelligence, had to develop such a plan four years after China.

The United States needs to win the microelectronics, 5G, and AI battlegrounds and make sure it is not caught by surprise again. Right now, we cannot confidently say that the United States is better positioned to proactively address “the next 5G,” or avoid “the next chips dependence.” We want U.S. government officials working with private sector and international partners to shape the future, not constantly trying to avert strategic checkmates. The United States cannot continue to shoot behind the target on critical technologies, address them piecemeal, or only belatedly connect their impact to the future of geopolitics and democracy once the consequences are too obvious to ignore.

The Geometry of Innovation Has Changed; the United States Has Not Adapted. The battlegrounds tell the story of a larger paradox of a techno-economic superpower suffering from strategically significant technological vulnerabilities. On the one hand, the United States can claim enormous companies with huge platform reach around the world, a rich tech startup ecosystem, the world’s leading chip designers, and innovation hubs sprouting beyond Silicon Valley. It still serves as the destination for global tech talent, and hosts the best universities. In even more basic terms, an economy seeking to lead in technology production needs inputs like capital and a productive workforce; a complex innovation system; and a home market large enough to support innovative enterprises at scale. The United States has it all. On the other hand, a withering technology manufacturing base, a stream of evidence that the U.S. military struggles to adapt leading technology for defense purposes, and a general paralysis on governing technologies like AI even as the EU and others move ahead, suggest something is amiss in the U.S. innovation ecosystem.

Why have these weaknesses emerged? There are many reasons. Here are a few. The tech ecosystem evolved without reference to a geopolitical rivalry and with relative indifference to the strategic implications of tech developments. High margin and high value chain investment and the search for cheap suppliers abroad made good business sense for U.S. companies and investors but devastated the U.S. technology manufacturing landscape. The absence of national technology priorities, and a decline in the share of government funded R&D left commercial priorities to drive the tech agenda. The absence of a modern “moonshot” left no concentrated national effort. And the bigger underlying

5 Kai-Fu Lee, [AI Superpowers: China, Silicon Valley, and the New World Order](#), Houghton Mifflin (2018).

issue is the changing geometry of the innovation ecosystem. The rise of venture capital (VC) reshaped the Vannevar Bush innovation triangle between government, industry, and academia, reducing the government's influence. VCs jolted the innovation landscape but largely stayed away from “deep tech” and tried to commercialize basic R&D – both of which required enormous patience and less promise of big returns.

The United States cannot rerun the Cold War playbook and hope it works, because conditions have changed. Rebuilding U.S. strengths and getting ahead of the next wave of technology requires mastering a new geometry of American innovation and harnessing it for national advantage. We cannot rest on the laurels of a strong technology ecosystem, a vibrant private sector, or superior ideals to naturally adapt. A passive U.S. approach to competitiveness based on the assumptions of a previous era leaves us with real vulnerabilities in this tech-enabled competition. We must think, act, and organize to compete by adapting enduring strengths to new challenges and new purposes. We must gather these strengths to compete.

Tech Trendlines are Concerning. The United States is not the world's sole technology superpower. China's technological progress is undeniable. The PRC is organized to harness technology for its economic, societal, and military ambitions, and it is backing up plans with resources. In 2019 alone, China spent nearly \$250 billion on its industrial policies.⁶ Anticipating the massive potential of data to create economic value and control society, the PRC is racing ahead with an ambitious digital strategy and a \$2.7 trillion campaign to build digital infrastructure.⁷ In looking at the key dimensions of technology competition, a picture emerges of an intensifying challenge. It is entirely possible to imagine a future where systems designed, built, and based in China dominate world markets with innovative, inexpensive, and centrally-controlled hardware, networks, and platforms; and where China is the leader in deep tech like AI, automation, synthetic biology, new energy, and quantum. History suggests that the nations capable of harnessing these technology waves are best positioned to win the future.

- *Sector Competition.* Broad sectoral strength matters because it is the basis for specific commercial and national security applications. It is always hard to assess U.S.-China “gaps” in dynamic technology sectors with multiple drivers, but it is clear that China has edged ahead in R&D and applications within several important

6 See for instance, Made in China 2025, the Dual Circulation Strategy, National AI Plan, the National Semiconductor Plan, Military-Civil Fusion, the Digital Silk Road. See also Gerard DiPippo, et al., [Red Ink: Estimating Chinese Industrial Policy Spending in Comparative Perspective](#), Center for Strategic International Studies (2022).

7 Barry van Wyk, [New Backbones for 'New Infrastructure' – China's Multi-Trillion Dollar New Digital Landscape](#), The China Project (2022). David Dorman, [China's Plan for Digital Dominance](#), War on the Rocks (2022).

technology sectors and intends to lead in all of them. In our judgment, China leads the United States in 5G, commercial drones, offensive hypersonic weapons, and lithium battery production. The United States has modest leads in biotech, quantum computing, commercial space technologies, and cloud computing, but these could flip to the China column. In the AI competition, the United States has a small lead with China catching up quickly across the AI stack.⁸ In all critical emerging technology sectors, China is making massive investments to catch up or take the lead.⁹

- *Platform Competition.* As tech platforms become tools of statecraft too powerful to ignore, China is redoubling its strategic play to win what many U.S. stakeholders had mistakenly seen as a purely commercial contest. These platforms have the power to facilitate content, decide what information is shared, how quickly and loudly it is amplified, and who has access to it. In possession of troves of data, digital platforms can help derive penetrating insights about global trends – and specific individuals. Chinese apps like TikTok, WeChat, and AliPay pose a threat to the dominance of U.S. counterparts in global markets. As physical, digital, and biotechnical technologies converge over the next decade, the platform statecraft competition will similarly expand beyond the digital realm.¹⁰
- *The Future of the Internet.* The Internet is being reshaped. A central question is whether the Internet will remain an open space for free expression and the exchange of information and services, or whether physical borders and government control will be replicated in the digital realm. Autocratic governments are building national firewalls. China is pushing to build global telecommunication architectures from undersea cables to 5G networks. The governments in two of the three largest democracies – India and Indonesia – are asserting intrusive control over the flow of digital information. Meanwhile, the Internet’s technological evolution is a wildcard in this contest as the push for a decentralized “web3” built on blockchain technologies could create a new paradigm for restoring a free Internet, fizzle out, or be similarly susceptible to government control.¹¹

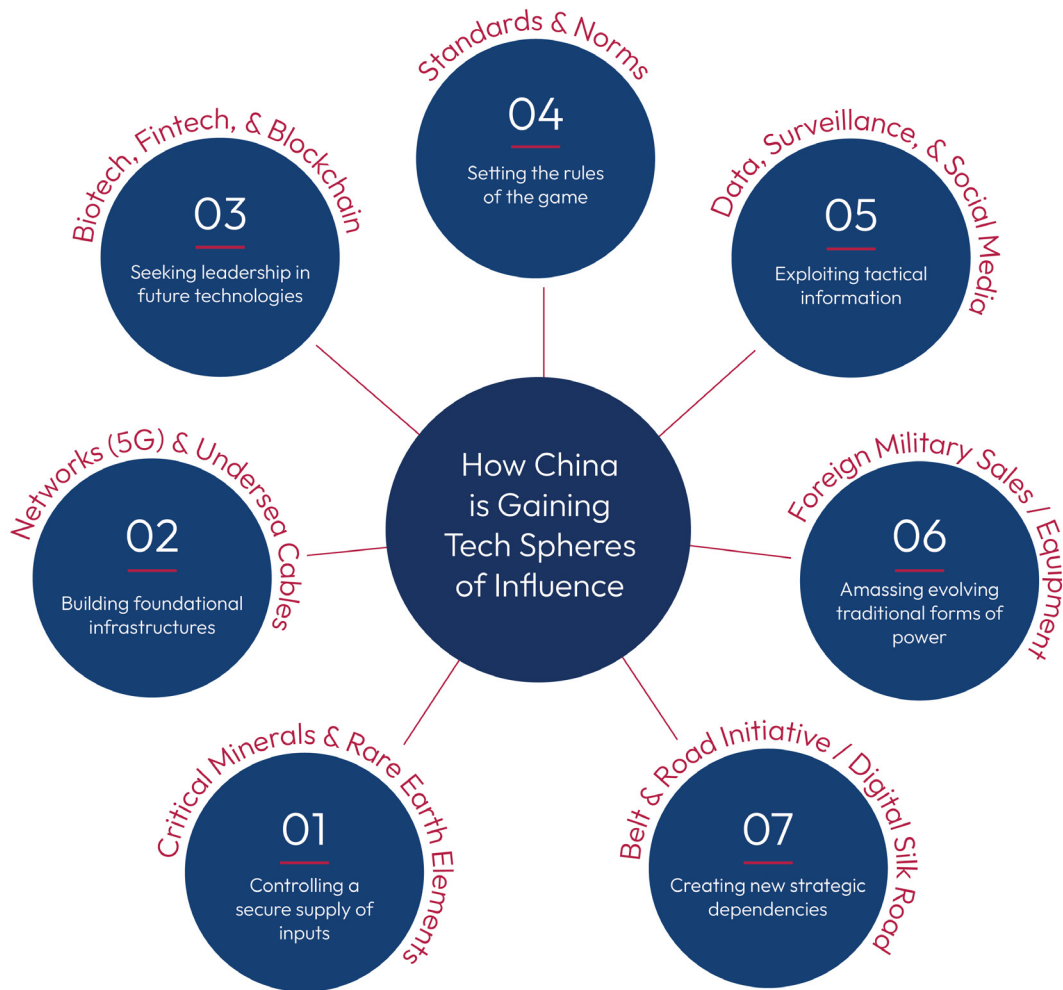
8 The National Security Commission on Artificial Intelligence defined AI as a stack requiring talent, data, hardware, algorithms, applications, and integration. See [Final Report](#), National Security Commission on Artificial Intelligence at 32 (2021) (citing Andrew W. Moore, et al., [The AI Stack: A Blueprint for Developing and Deploying Artificial Intelligence](#), Proc. SPIE 10635, Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR IX, 106350C (2018); Dave Martinez, et al., [Artificial Intelligence: Short History, Present Developments, and Future Outlook](#), MIT Lincoln Laboratory at 27 (2019)).

9 SCSP acknowledges that a robust public dialogue exists related to comparing the progress of the United States and China on critical technology sectors, with many perspectives on the state of play and each nation’s progress. This report provides our initial assessments – based on a broad assessment of data, trends, and expert views surveyed to date.

10 See Chapter 7 of this report for discussion of physical, digital, and biotechnical technologies on the horizon.

11 See, for example, [The Unlimited Potential of Web3 with Alexis Ohanian](#), Where it Happens (2021); Moxie Marlinspike, [My First](#)

- China's Growing Tech Spheres of Influence.* China's tech advantages are translating into strategic impact through the classic idea of spheres of influence applied through new methods and in new domains. China's spheres of tech influence range from control of critical inputs like rare earth minerals to network infrastructure through its Digital Silk Road projects, strategic approach to international standards bodies, and export of surveillance technologies. This tech influence is translating to geostrategic leverage around the globe as countries dependent on China vote differently in international bodies, change their position on Taiwan, and toe the PRC's foreign policy lines on issues ranging from human rights to cyberspace norms.



Beijing's Counter Narrative. China's leaders claim the future is theirs. These trends feed the narrative that the trajectory is inevitable. America's problems, they claim, are part of

[Impressions of Web3 \(2022\).](#)

a broader “disorder of the West,” presaging “the end of the ‘end of history.’” Democracy is in retreat. The United States’ technology advantages are withering, its private sector isn’t public-minded, and its public sector is too paralyzed to act. Economic power is shifting from West to East. The United States’ military advantages have eroded. Meanwhile, China, according to its leaders, has unlocked the secrets of winning the 21st century. It is delivering opportunities for its people to lift their lives. The Chinese Communist Party (CCP)’s plan for the “great rejuvenation of the Chinese Nation” is on track, and the PRC is now the “main driving force” behind the world’s technological and industrial transformation. Its socialist approach “with Chinese characteristics” represents “a brand-new possibility for achieving modernization.”¹² As President Xi told President Biden: “Democracies cannot be sustained in the 21st century. Autocracies will run the world.”¹³

Why 2025-2030. 2025-2030 represents a critical window where tech trends and strategic competition will come to a head in the contest. If we want to alter the trajectory of the competition, we must organize now.

Key aspects of Beijing’s comprehensive plan to bolster its military capabilities and execute its techno-economic strategy must succeed during this decade. Between now and the end of this decade is a window of opportunity that will quickly close for China as its demographic and economic trends darken unless technology provides an escape ramp.¹⁴ Economic headwinds in 2022 – “Zero-COVID,” supply chain shocks, and localized financial turbulence – may be accelerating that window’s close. Notably, the People’s Liberation Army (PLA) is building the capability to mount a full-scale invasion of Taiwan, should CCP leadership decide to do so this decade.¹⁵ Because China’s leaders know the window will close, the PRC appetite for risk may increase before 2030.

- We are entering a key period of competition to determine which companies and nations establish, adopt, and scale the dominant technology platforms emerging from rapidly maturing general purpose technologies beginning with AI, biotech, quantum, and novel energy paradigms.¹⁶ On the digital front, much of the world will be integrated into a new world of IoT with 5G-enabled sensors, autonomy,

¹² [Translation of The World is Undergoing Great Changes Not Seen in a Century; What are these Changes?](#), Center for Security and Emerging Technology (2021).

¹³ [Remarks by President Biden at the United States Naval Academy’s Class of 2022 Graduation and Commissioning Ceremony](#), The White House (2022).

¹⁴ Welcome to the Machine: A Comparative Assessment of the USA and China to 2035 Focusing on the Role of Technology in the Economy, Fathom Financial Consulting at 3 (2022) (*SCSP-commissioned work product*).

¹⁵ Sam LaGrone, [Milley: China Wants Capability to Take Taiwan by 2027, Sees No Near-term Intent to Invade](#), US Naval Institute News (2021); Derek Grossman, [Taiwan is Safe Until at least 2027 but with One Big Caveat](#), RAND Corporation (2021).

¹⁶ See Chapter 7 of this report for further discussion of general purpose technologies.

and connectivity underscoring the importance of who will build and fundamentally control the digital infrastructure that impacts every aspect of human existence.¹⁷

- The EU, China, and others are actively developing the regulatory landscape for the digital world, AI, and other technologies, while the United States continues to debate a national approach and relies instead on a patchwork of local and state laws and voluntary frameworks. Without a clear strategy on tech governance – including to rally allied support behind its approach – the United States risks being bound to a global innovation landscape shaped by regulatory regimes decided in foreign capitals.
- At home, 2025 will be an opportunity to initiate the next phase of competitive strategies. It will mark the beginning of a second Biden Administration or the start of a new administration. We will have a better sense of the progress of initial efforts to rebuild microelectronics manufacturing at home, restore supply chain resilience for critical minerals, and provide alternatives to China’s 5G expansion. The United States will need, at that point, the next set of policy recommendations ready to carry a technology competitiveness agenda forward. As a practical matter, we have just one full congressional legislative cycle between now and then. To improve the U.S. position by 2025, we must act now.

Remembering American Advantages. The window for action to shape the future is still very much open. The question we must ask is how to harness American strengths. No single public policy action or technology solution will be sufficient. However, the basic elements for a strong response exist.

- *America’s open society provides political, economic, and cultural advantages.* Innovation happens in America because an open society inspires, facilitates, and attracts talent to achieve the next generation of technology breakthroughs. It is a culture rooted in the free exchange of ideas that supports scientific breakthroughs and business opportunities.
- *The United States is a global talent hub.* By leading the world in higher education and offering an open innovative society, it can attract the world’s best talent. The nation’s values and open society make it a welcoming destination for all. The United States is constantly replenishing a strategic reservoir of human capital.
- *American financial dynamism is unparalleled.* The United States draws on the world’s deepest and most liquid capital markets to generate prosperity and turn

¹⁷ Shankar Deka, et al., [Towards Cyber-physical Systems Robust to Communication Delays: A Differential Game Approach](#), arXiv (2021).

ideas into products and platforms at home and around the world. U.S. legal and regulatory institutions have long been the reliable backstop of an efficient and dynamic ecosystem that supports cutting-edge research, development, and commercialization.¹⁸

- *America is primed for moonshots.* If the U.S. Government steps forward to set grand technology objectives, it can spur national enthusiasm, galvanize the private sector to action, and accelerate innovation in strategic sectors. These attributes also enable the innovation ecosystem to constantly reinvent itself. Today novel funding paradigms and a decentralized “crowd” (in science and finance) could fuel additional new discoveries.

Three additional features will help translate advantages for the age of tech competition.

- *Innovators and investors recognize the growing international competition.* Silicon Valley is undergoing a sea change. The space for private-public collaboration is expanding as a growing segment of the private sector recognizes and wants to respond to tech-based challenges to democracy, particularly from foreign rivals.
- *Technology innovation presents an opportunity to harness America’s diversity.* Engaging a rising, diverse generation of technology leaders not only draws on a wider pool of talent and ideas, but also offers the chance to build more equitable and inclusive technologies that help America better live its values and demonstrate its power to the world.
- *A global network of allies and partners share U.S. strategic concerns and are committed to deepening tech cooperation.* America is not competing alone. Allies and partners can tip the balance in a close race, nearly doubling the scale of research and development spending when combined with America.¹⁹

We Have Been Here Before. At every critical phase of American history, enduring principles – the centrality of individual rights, the power of free enterprise, and the strength of democratic governance – have been tested by international forces, technological disruption, threats from abroad, and our own domestic struggles to reconcile our principles and our practices. Through the transition from an agricultural society to industrial engine and digital superpower, and a global ideological and strategic contest in the Cold War, we have passed the tests – albeit painfully – and built a stronger and freer United States. We sometimes fell short in living up to our ideals, but that disconnect was not an excuse to

¹⁸ See Chapter 2 of this report for a discussion of the history of industrial strategy in the United States.

¹⁹ Melissa Flagg, [Global R&D and a New Era of Alliances](#), Center for Security & Emerging Technology at 3 (2020).

abandon competition or a reason to jettison principles.

Today, we must retain confidence in our advantages and our enduring values. We can adapt without abandoning our core beliefs, evolve without sacrificing our values, and exercise our power abroad without losing sight of its purpose. If we can harness the wave of new technologies, then we will put the United States in a stronger strategic position in the world, create a healthier, innovative society with expanding equality of opportunity at home, and present a democratic model worthy of emulation abroad. Success depends on building national consensus on the problem, taking the actions necessary to restore all dimensions of U.S. competitiveness in the world, rebuilding a system of alliances and international order, and adapting our society and economy by harnessing technology to solve practical problems. We know we need to act, but we must agree on how we can win.

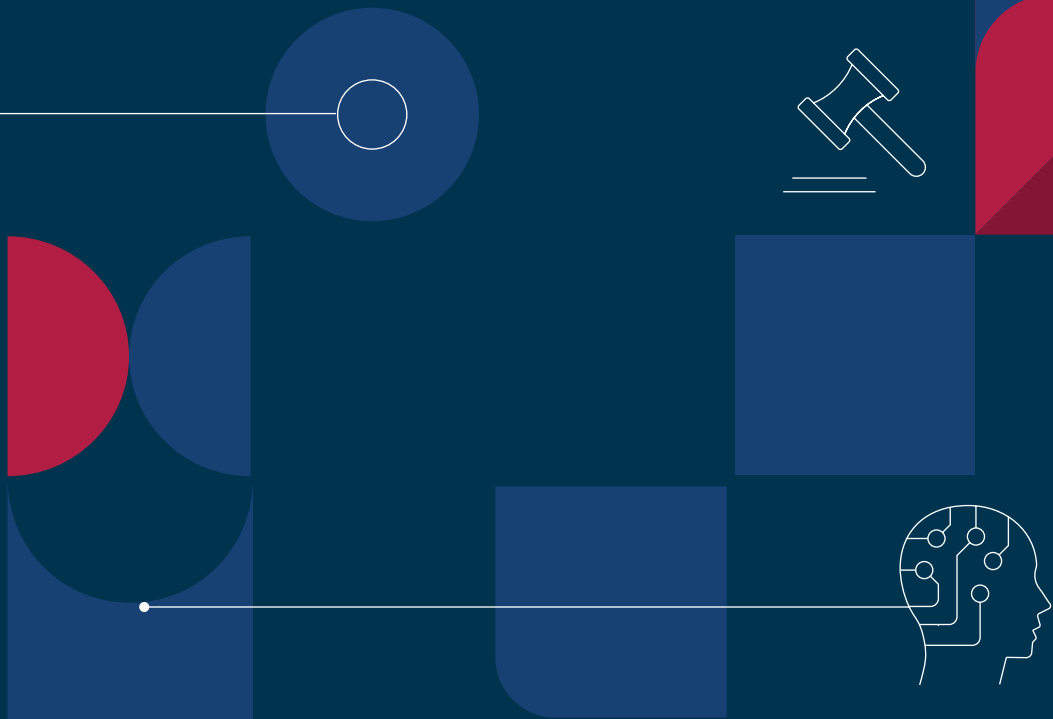
The Six Challenges the United States Must Win

Mid-Decade Challenges to National Competitiveness





- **Harnessing the New Geometry of Innovation**
- **Restoring the Sources of Techno-Economic Advantage**
- **An American Approach to AI Governance**
- **Remaking U.S. Global Leadership in the Age of Technology Competition**
- **The Future of Conflict and the New Requirements of Defense**
- **Intelligence in an Age of Data-Driven Competition**



A COMPETITIVENESS AGENDA

The Six Challenges the United States Must Win

The United States can be on a winning path by the middle of the decade if it can solve six challenges. The cumulative answer to how we address these challenges constitutes an agenda for restoring America's competitiveness.

The first three challenges are foundational to *how* the United States pursues technology innovation – through a national process to identify and accelerate promising breakthroughs, a techno-industrial strategy that translates technology advantage into economic power and prosperity, and an American way of tech governance that supports innovation by accounting for risks and bolstering public confidence. Fundamentally, this represents a plan to shift the U.S. approach to tech competition from reactive and defensive to strong and agenda-setting. The last three challenges address the foreign policy, defense, and intelligence instruments of American statecraft that protect and extend national competitiveness in a global context. Technology competition is changing the geopolitical landscape; the tools to compete must adjust.

The chapters that follow elaborate on each element of this agenda to identify key issues within each that, if addressed, can change the competitive landscape in America's favor.

Challenge 1: Harnessing the New Geometry of Innovation

How can we unlock and connect the expertise, will, and resources that exist throughout American society to build national advantages in critical technologies? The United States' strengths across its commercial, academic, and government sectors are not oriented for international competition. Our proposed answer is a new public-private model – one that

provides a focused strategy process for the United States to deploy in making informed judgments on national technology priorities and for creating action plans to accelerate the tech applications.

The United States cannot continue to shoot behind the target on the next critical technologies, such as biotechnology, smart manufacturing, and new energy production and storage. Without a national plan, the United States is set to address them in a piecemeal fashion, or only belatedly connect their impact to the future of geopolitics and democracy once the consequences are too obvious to ignore. This dynamic has led to ongoing, belated U.S. efforts to rebuild its microelectronics industry, prevent domination of global 5G infrastructure by companies backed by a rival state, and extend U.S. leadership in AI. In each case, the United States was caught flat-footed and had to respond to mitigate real strategic disadvantages. Across two presidential administrations, policymakers acted boldly in these three tech areas, but in reaction mode. We cannot confidently say that the United States is better positioned to proactively address “the next 5G.” Even if our awareness of the tech-national security nexus is heightened, unless something changes we will continue to play strategic tech whack-a-mole. Looking out to 2030, we must act soon to anticipate trends and get ahead of them. The competition for paradigm-altering general purpose technologies is intensifying and expanding to new areas.

In Chapter 1, we offer a new public-private model of cooperation that outlines an organized process for getting past listing important sectors to curating and resourcing investable options for technologies that can drive national competitiveness. First, the United States is home to some of the world’s best tech horizon scanners, and those nodes of expertise should be linked into a network to support national goals. They should be guided by an evaluation framework that systematically analyzes the significance of a given technology, whether U.S. rivals are positioned for advantage, and what needs to be done to improve the U.S. position. Second, identified key technologies require action plans that push beyond mere lists of important technology sectors to set concrete goals for investing in, incentivizing, and accelerating the development of specific capabilities. Third, public and private resources should be blended through resourcing mechanisms that can accelerate innovation and fill international competition gaps.

The United States lacks a hub to coordinate and undertake these activities. Several viable options exist — and are worthy of study — based on possible paths in the executive and legislative branches, as well as via new public-private arrangements. An entity, or combination of entities, dedicated to enhancing America’s technological competitiveness should serve three primary functions: coordinate both within the government and between

public and private stakeholders, provide original analysis to support decision-makers, and operate as an action arm to implement action plans that move strategic technologies forward. All three functions need not sit under one roof. But establishing a lasting and integrated set of actors would best support long-term strategy across a multi-decade competition.

Over the past year, SCSP has prototyped the kind of technology evaluation process we are proposing by convening leading figures from across American society. Based on that work, our preliminary judgment, discussed in Chapter 7, is that AI, novel computing paradigms, and new networks will remain as battlegrounds between now and 2030, while biotechnology, new forms of energy generation and storage, and new manufacturing paradigms will join as must-win competitions. Within these and other fields, our early analysis has identified several specific and audacious technology goals that the United States should advance through an organized strategy.

This next wave of innovation will stitch together the physical, digital, and biotechnical realms. For example, AI is driving advances in drug discovery, chemistry, and fusion energy. Synthetic biology is expanding beyond health to transform sectors such as agriculture and materials. Computing may be transformed through neuromorphic, biological, and quantum methods. Next generation networks will shape the digital domain's links with the physical and biotechnical, as 6G, blockchain, and quantum communications evolve. And breakthroughs in energy storage, such as new battery chemistries, and in energy generation, such as nuclear fusion, could revolutionize how we travel, how we build, how we compute, and how we protect our environment. The convergence of multiple general purpose technologies could lead to a broad reinvention of America's manufacturing base.

Challenge 2: Restoring the Sources of Techno-Economic Advantage

How do we ensure that the United States remains the world's most dynamic, competitive, and resilient economy in the 2020s? America's advantages across its innovation ecosystem, workforce, and financial sector mean the economic competition should be America's to lose. Today, however, the erosion of American manufacturing combined with the PRC's techno-economic advance has triggered anxiety that the American system lacks resilience and cannot convert its advantages into national power. As Chapter 2 elaborates, to stay ahead, the United States needs a techno-industrial strategy that increases economic output and fills economic and national security gaps.

Despite holding advantages across key economic fundamentals, the United States is falling

behind in advanced industries.¹ Government inattention has led to companies outsourcing much of their manufacturing to East Asia, resulting in an imbalanced U.S. economy with advantages in software but vulnerabilities in manufacturing. The United States is losing the ability to produce critical technology inputs and remains reliant on supply chains that run through or dangerously close to its main strategic rival.

Secure access to critical technology inputs is a cornerstone of national competitiveness. Leverage over the raw materials, production capacity, and know-how required to build components of digital networks, high performance computers, defense systems, electric vehicles, and virtually every other significant piece of modern technology is a freshly appreciated source of power. The location of hardware manufacturing, once an afterthought in a globalizing world focused on software innovation, is becoming critical to strategic competition.² The CCP's strategy is to capture the entire value chain of key inputs, including permanent magnets, batteries, and semiconductors, to reduce its own strategic vulnerability and build leverage to exercise abroad. In such a world, ceding lower levels of the value chain means accepting serious strategic risk unless the locations and supply chains for the critical technologies can be secured.

To address these vulnerabilities, the United States must double down on its strengths. "Industrial policy" is a fraught label, but targeted government intervention can fill critical gaps and provide public goods when the market falls short. Building digital infrastructure and strengthening the American workforce, for example, can create a path for technologies to diffuse across the economy, unleashing private sector innovation and boosting economic output. Public-private partnerships can help the United States address its supply chain vulnerabilities and preserve financial leadership by unlocking innovation in digital finance.

Investment at home is not enough. Beijing's systematic technology theft and massive government support for strategic industries have destroyed the idea of a level playing field, leaving firms in the United States and allied countries at a disadvantage. Inadequate guardrails on capital flows and the export of dual-use technologies mean America and its allies are funding and supporting the PRC's technology ambitions and military modernization. Pushing back is a necessary step towards restoring democratic techno-economic advantage.

Ultimately, the question is which system is better organized to convert economic

1 Robert D. Atkinson, [The Hamilton Index: Assessing National Performance in the Competition for Advanced Industries](#), Information Technology and Innovation Foundation (2022).

2 Taiwan is the center of the microelectronics universe, making it a fulcrum of techno-economic competition. The Netherlands, because of one company producing exquisite ultraviolet lithography equipment critical to the most advanced chips, is a chokepoint in the PRC's ambitions and a unique source of Western advantage.

fundamentals into enduring national advantage. This calls for a five-part techno-industrial strategy to ensure a more prosperous and resilient U.S. economy. The first and second elements are investing in digital infrastructure and developing a tech-savvy workforce, including by attracting talent from abroad. Third is building manufacturing capacity for critical inputs. Fourth is preserving U.S. global leadership in finance, including by leveraging innovations in digital finance. Finally, the United States needs to wield its economic and financial might to curb the PRC's techno-economic malpractice.

Challenge 3: An American Approach to AI Governance

How can we develop a technology governance regime that protects the rights of individuals and still unlocks the power of innovation to improve society? All societies are searching for models of technology governance that enhance global competitiveness by propelling innovation while also accounting for risks and vulnerabilities. The EU is building a regulatory framework. China is pioneering a techno-authoritarian model. The search for an American model, outlined in Chapter 3, takes place in this global context.

Tech disruptions have impacted the relationship between state and citizen, introduced novel governance dilemmas, and enhanced the vulnerabilities of open societies to external threats. Public concerns about these challenges need to be addressed for the United States and other democracies to fully capitalize on broad societal benefits that the tech revolution promises – to improve public health, for example, or to better manage the environment. Prevailing in a contest of political systems requires finding greater consensus, within and among democratic states, on how to resolve the democracy dilemmas of the digital age.

The digital revolution is challenging foundational principles of America's constitutional system of government – especially privacy, free speech, and equal protection. Modern business models that thrive on personal data have prompted intense concerns about how that data is controlled and traded, yet numerous proposals for national legislative frameworks have stalled. New surveillance and facial recognition technologies are enhancing the investigatory powers of the state, yet clear restrictions and guidelines have been piecemeal. The question of online content moderation remains mired in disagreement over approaches to intermediary liability. And while the turn to automation is improving efficiency across many sectors, algorithms are appearing to reinforce human decision-making biases in contexts as wide-ranging as hiring, home loan approvals, and health care. The prospect of further policy paralysis on all of these fronts risks eroding public trust and hindering innovation.

Given the vulnerabilities of open societies to external interference, some of these

governance challenges also present national security problems. Competitors are exploiting digital dependence across society through cyber-attacks, data harvesting, and sophisticated disinformation campaigns. Democracies are especially vulnerable due to their openness, decentralized approach to connectivity and digital governance, absence of centralized infrastructure protection, patchwork rules on data privacy and security, commitment to the free exchange of information and ideas, and tolerance for strategic competitors' companies to operate relatively freely in our digital realm.

For AI, which presents the most consequential and far-reaching governance challenges in the near term, four principles should guide the American approach. First, the United States should take a sectoral approach because the risks and opportunities of AI are inextricably tied to the context in which it is used. Second, the United States should rely primarily on existing regulatory agencies, which have experience incorporating rules for new technologies. Third, governance should focus on high consequence use cases. Finally, in addition to regulatory guardrails, the United States should utilize robust non-regulatory approaches to governance.

These principles should inform an agenda focused on several priority areas for governance. Data privacy rights are critical to a digital future aligned with democratic values. We need to forge a new consensus on the pre-digital legal concept of a reasonable expectation of privacy. Facial recognition concerns should be tackled through targeted use-case restrictions. We need to operationalize the principle of mitigating unwanted bias in AI systems and ensure there are options for recourse when systems prove unfair. We need better ways to anticipate socio-technical consequences of AI systems prior to their use. And social media platforms need a multifaceted approach to mitigate disinformation.

Tackling this agenda can make room for greater attention to ensure that promising tech breakthroughs are marshaled to improve lives more broadly. This promise can be seen in tech solutions for more effective government — smart cities, better and safer transportation, and efficient social services. The promise is evident in human health and environmental stewardship. Consider recent AI-driven advances in personalized and precision medicine, gene therapy, vaccine discovery, drug design, and cancer screening. Or advances in environmental solutions, including optimized crop management, reduction of plastic waste, and experiments with fusion energy. If we consider the wide application of AI across sectors, effective U.S. leadership in AI and data governance is imperative to shaping our society in 2025 and after. The lessons we learn from governing AI will set precedents for governing other emerging technologies as well.

Challenge 4: Remaking U.S. Global Leadership in the Age of Tech Competition

How can we preserve an open international order, underpinned by respect for sovereignty and trusted digital infrastructure, that meets the aspirations of the widest number of people and is still guided by democratic values? Chapter 4 traces technology's place at the heart of the long-term contest between democracy and authoritarianism. The PRC is pursuing a methodical approach to build technology spheres of influence from which it can coerce political preferences. Its strategy rests on controlling the global digital backbone, providing useful platforms and services, and setting international tech standards. The United States and its allies must marshal the resources and diplomatic efforts to compete across the world so nations have real choices about their futures.

The Internet is now as significant as any piece of physical geography – democracies will need to double down on technological solutions and technical standards-setting that support an open, interoperable, and secure Internet against PRC-led authoritarian efforts to close off digital borders and extend the surveillance and censorship power of the state. The protection of digital freedoms is intertwined with the physical pipework beneath it. The world's digital infrastructure is the new key to global influence. Whoever controls the digital infrastructure that moves and stores data determines the security of data flows, the global centers of economic prosperity, and the values of the society that it connects. Democracies must organize and cooperate to build secure, trusted, and resilient wireless networks (especially 5G and its successors), cables (both terrestrial and undersea), operating systems, data centers, and the digital apps, software, and platforms that support everyday governance, commerce, and life.

Most nations do not want to choose between the United States and the PRC nor see their choices as part of a contest between democracy and autocracy. The alignment of these “swing states” in the larger rivalry, which can tip the balance of winning to one or the other, will be determined by their own multi-layered definition of national interests. A winning strategy requires convincing much of the world that secure, trusted digital technologies serve their own interests, not only the United States' and its allies' geopolitical goals, and that authoritarian tech is a threat to their sovereignty. And it involves ensuring cost-effective and quality alternatives exist.

No democratic nation – not even the United States – can win this competition on its own. We will need to develop techno-industrial strengths within a cooperative alliance agenda, recognizing that the technology competition is not simply about economic advantage but also a national security challenge that affects us all. The United States will need to leverage the strength of the technology platforms that the dynamic private sector brings to the

competition. And we will need a U.S. Government that is organized to pursue a foreign policy to win the tech competition. Success hinges on the United States' ability to overcome the advantages in scale and speed of national action that the PRC system brings to the tech competition. As the competition intensifies and we enter a more bifurcated world, the United States will need to construct a new relationship with the PRC to mitigate the risks of escalation that includes continued engagement with its citizens.

Challenge 5: The Future of Conflict and the New Requirements of Defense

In the face of military rivals employing new technologies and operational concepts to gain advantage, how can the United States ensure a favorable global balance of military power, and uphold its defense commitments in the event of an aggression? A strong military deterrent to keep the peace is a necessary precondition for pursuing a positive agenda. Chapter 5 sketches the interplay of new technologies and traditional geopolitical rivalry that are producing a dangerous set of international conditions.

The character of warfare is changing. Already, we are in a new era of persistent cyber, economic, and information conflicts below the level of overt combat that risks bringing us closer to direct confrontation. Emerging technologies are changing the range and specificity of effects, enabling the microtargeting of individuals, and qualitatively changing the way we communicate, perceive our environment, and make decisions.

The PLA has closely studied the “American way of war” which they refer to as “informationalized warfare.”³ The United States was the first mover, giving it an unmatched military-technical advantage that lasted from the end of the Cold War to now. Both China and Russia have been intent on achieving military-technical parity with the United States in this style of warfare, and they have largely succeeded. This will make any future American power projection operation far riskier and will undercut our conventional deterrent posture.

The application of new technologies to conflict and changes in the military balance of power have engendered doubts about the U.S. military's capacity to maintain its defense commitments, and with it the credibility of the U.S. deterrent. This can create a window of vulnerability in which rivals will be tempted to employ military force to achieve their objectives. China is actively seeking to harness new defense technologies to erode or surpass the U.S. military's capabilities. This challenge is compounded by the brittleness of America's own defense industrial base, the gradual nature of the U.S. military's transition from legacy capabilities to cutting-edge systems, and the struggle to adopt novel

³ Informationalized warfare combines guided weapons of exceptional range and accuracy and the “battle networks” that provide them with precision targeting information. The Chinese refer to battle networks as “operational systems,” and see future warfare against large peer competitors as an era of “systems confrontation.”

operational concepts. These dynamics have produced a growing threat to peace and stability in the Indo-Pacific, the most strategically critical region of this century.

The United States should respond neither with despair nor hubris. We retain significant military-technological advantages that we can continue to leverage. Demonstrated experience in joint operations, empowerment of warfighters at the lowest level, hardened expeditionary logistics for contested environments, cultivation of both traditional and new allies and partners, and maintenance of a highly professional military – to name a few – remain critical U.S. advantages that China will struggle to replicate quickly, if at all.

To improve America’s military position, we outline a new competitive approach – which we call the Offset-X strategy – which would help the United States circumvent China’s military advancements and concepts of operation, restore America’s ability to more freely project power in the Indo-Pacific, and position the United States to honor its commitments to the stability of the region. This approach centers around several areas of focus, including distributed and networked operations, human-machine collaboration, human-machine teaming, primacy in software-centric warfare, resilience, and greater technological interoperability and interchangeability with allies and partners. Through these initiatives, the U.S. military will be better prepared and positioned to outsmart, outpace, outmaneuver, and – as necessary – outgun the People’s Liberation Army.

Challenge 6: Intelligence in an Age of Data-Driven Competition

How can the United States win the race for actionable insight in an information-rich and geopolitically-competitive world? Out-knowing authoritarian rivals is a critical advantage in strategic competition. Chapter 6 describes how the U.S. Intelligence Community (IC) will have to master emerging technologies to deliver relevant and timely insight to decision-makers, and augment its efforts by focusing on foreign technology developments shaping military, economic, and political trends.

Today, the IC is still transitioning between countering terrorism and supporting geopolitical competition. For the next decade, the rivalries with China and Russia, more than any other security problems, will shape what U.S. leaders ask of intelligence agencies, and how intelligence officers must operate to collect and process information consumers need.

Digital technologies are rapidly changing the intelligence environment. As foreign adversaries and private companies gain new capabilities, U.S. intelligence organizations risk falling behind. Intelligence collection has become harder. The rapid advancement of adversarial capabilities at a global scale jeopardizes the IC’s long-term effectiveness. As the PRC builds out digital infrastructure globally, U.S. intelligence will more frequently

operate in environments where Beijing will have visibility into their physical and digital trails. Many pertinent insights reside within the private sector. Policymakers are turning more frequently to commercial companies to deliver. Once-unique capabilities, like geospatial and signals intelligence, have been commercialized. Private companies are often better positioned to exploit AI and other technologies for their products.

The IC's ability to rise to the occasion will hinge on whether it can adapt to the new technological era through digital transformation; leverage a dedicated, tech-driven, open source organization to support U.S. decision-making; create new capacities to capture and master foreign economic, financial, and technological intelligence; and counter foreign threats in the information domain.

Harnessing the New Geometry of Innovation

Mid-Decade Challenges to National Competitiveness

01





- The Process

- A Framework for Ascertaining a Technology's Strategic Significance

- Studying the Horizon

- Curating the Platforms of the Future

- Mobilizing the Entrepreneurs of American Advantage

- Organizing the Government-Private Sector Nexus



CHAPTER 1

Harnessing the New Geometry of Innovation

The United States almost missed the strategic significance of developments in microelectronics, 5G, and AI – the current three biggest tech battlegrounds – because no one in government was responsible for identifying strategically relevant technologies and making sure the United States had a plan to build them. The battlegrounds are at-once competition stories, prerequisites for future technology sectors, and microcosms of bigger issues confronting the nation. They reveal that the United States still has no process or person responsible for achieving technology advantage. Going forward, America must be able to get ahead of the target in defining critical technologies. Looking to 2030, the United States must both maintain its focus on microelectronics, wireless networks like 5G, and AI, and prepare to act on still-emergent sectors – “the next 5Gs” – that will reshape our lives and drive long-term competition with China.¹ Doing so requires mastering the new geometry of innovation.

Following the Second World War, the United States seized a lead in advanced technologies by understanding and leveraging the scientific and industry landscape. Guided by Vannevar Bush’s vision in “The Endless Frontier,”² a knowledge-generating triangle of government, academia, and industry carried us to the moon,³ seeded Silicon Valley,⁴ and created the Internet.⁵ Yet, in only a few decades that triangle began to evolve, and the role of government in setting and driving the agenda for new scientific frontiers began to diminish. Silicon Valley and modern venture capital grew into a force of its own.⁶ More

1 For more on still emergent tech sectors see Chapter 7 of this report.

2 Vannevar Bush, [Science: The Endless Frontier](#), National Science Foundation (1945).

3 Arnold Levine, [Managing NASA in the Apollo Era](#), National Aeronautics and Space Administration at 71 (1982).

4 Margaret O’Mara, [The Code: Silicon Valley and the Remaking of America](#), Penguin Press at 17-29 (2019).

5 [From ARPANET to the Internet](#), Science Museum (2018).

6 Margaret O’Mara, [The Code: Silicon Valley and the Remaking of America](#), Penguin Press at 204-205 (2019); Sebastian Mallaby, [The Power Law: Venture Capital and the Making of the New Future](#), Penguin Press at 18-19 (2022).

recently, the information age opened the door to a fifth player – “the crowd”⁷ – that has bolstered individualized capacity to provide sources of funding⁸ and driven new research outside of traditional institutions.⁹ The innovation landscape has changed, but thus far America has not fully adapted.

In isolation, the United States’ failure to respond to the changed geometry of innovation would be unfortunate. In an international competition, it is a strategic vulnerability. The United States confronts a highly organized rival with a similarly sized economy that is tightly interwoven with its own.¹⁰ The competition’s stakes are high, and the market alone has not naturally aligned with the nation’s

The U.S. public-private ecosystem has vast competitive strengths, but they are ungathered. America needs **a plan for mastering the new geometry of innovation** to compete.

needs for that competition. Absent targeted action, the United States is unlikely to close the growing technology gaps with China by a strategy of chance. The U.S. public-private ecosystem has vast competitive strengths, but they are ungathered. America needs a plan for mastering the new geometry of innovation to compete.

A new public-private model would recognize the five power centers driving innovation and seek to harness them to gain advantage. The nation needs a process that puts that public-private model into action.

The Process. A national technology strategy process would unlock America’s latent power to compete in the sectors that matter most, enhancing the United States’ position while drawing on American strengths and remaining consistent with American norms.

- The United States must build a national process for horizon scanning for emerging technologies and rivals’ strategies that draws on a range of experts. Absent an international competition, recognizing innovation is important. In an international competition, it is vital. America possesses vast horizon scanning talent across

7 Clay Shirky, [Here Comes Everybody: The Power of Organizing Without Organizations](#), Penguin Press (2008).

8 Holly Else, [COVID “Fast Grants” Sped Up Pandemic Science](#), Nature (2021); Tyler Cowen, et al., [What We Learned Doing Fast Grants](#), Future (2021).

9 Sarah Hamburg, [A Guide to DeSci, the Latest Web3 Movement](#), a16z Futures (2022).

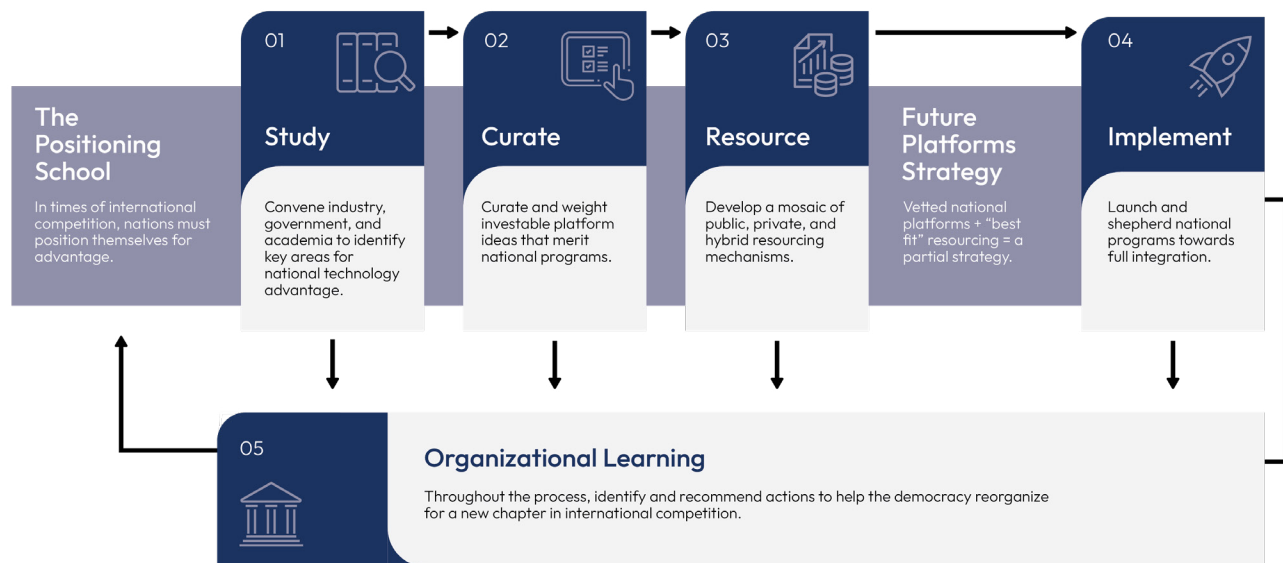
10 See Andrew Krepinevich, [Preserving the Balance: A U.S. Eurasia Defense Strategy](#), Center for Strategic and Budgetary Assessments at 38-39 (2017).

academia, industry, and government, but it has yet to link those expert nodes into a network that supports national goals.

- The United States must curate national action plans for strategic technologies that set bold technology goals and prime the ecosystem for diffusion and adoption. The nation needs an integrated process for evaluating necessary moves by creating “minimum viable solutions” that push beyond merely composing lists of important technology sectors toward concrete achievements and plans that benefit the entire nation – and often the broader world.
- The United States must marshal public, private, and public-private resources to put the appropriate focus behind bold technology goals. Many in the innovation ecosystem are waking up to the international competition and the risk that the United States may lose in it. The government and private sector can harness this latent potential to gain leverage in the international competition.

Even if this process represents the right equation for regaining tech advantage, the United States lacks a hub for implementing this process to devise and enact long-term technology strategy. The United States needs an organization that can lead in this effort by providing an action arm that is accountable, capable, and lasting.

National Technology Strategy Process



A Framework for Ascertaining a Technology's Strategic Significance

The nation requires a process for identifying and teeing up action on a select number of strategically significant technologies.

In international competition, nations unable to identify and prioritize strategic technologies for action will fall behind and suffer from the resulting vulnerabilities. Spurring select action plans that mobilize the ecosystem towards a positional advantage can help address novel threats from abroad, seize raw opportunities, and explore novel paradigms that change the way that the nation – and the world – performs scientific discovery, technology, and engineering. The path to action begins with a framework – shown below – that provides a nuanced, but accessible, lens for policymakers to find strategic signal amid the noise.

Defining essential national technology goals and marshaling resources for a technology move starts with understanding the technology itself. As the box on the left in the graphic below outlines, a set of technology questions helps assess an emerging technology's capacity to drive broader, fundamental change, and its potential impact on the economy, national security, and social structures. Next, as crafting a strategy in a resource-constrained world demands prioritization, a technology strategy framework considers rivals' positioning (middle box). A rival's lead – or possession of the resources, talent, and will to lead in a strategic technology – heightens the urgency of competing in that space. Finally, the framework looks inward (box on the right), probing the U.S. and allied ecosystems to understand their current state and needs for maintaining, bolstering, or supercharging American competitiveness through partnerships, investment, and harmonizing the regulatory and innovation environments.

In international competition, nations unable to **identify and prioritize strategic technologies for action** will fall behind and suffer from the resulting vulnerabilities.

Strategic Evaluation Framework

These questions can be used to find strategic signal in the noise to define national technology goals to enhance American competitiveness in the 2025-2030 timeframe.

Technology Factors

Is this technology strategically important enough to warrant fostering a dominant national position?

- Could this technology yield a revolutionary breakthrough that upends existing paradigms or fundamentally changes the way the world works?
- Is this a general purpose technology (GPT) like electricity that could subvert or accelerate many other sectors?
- Does this technology present or solve a novel, foreseeable, and material existential national security threat?
- Could this technology alter the economic fundamentals of the United States? Relatedly, does this technology or program present massive spinoff potential?
- Could this technology change the military balance of power outright by its existence?
- Could this technology transform the means of production of information and/or the control of its flow in society?
- Does this technology possess “first-mover” criteria such as scarce factors of production, network effects, or other forms of potential lock-in.

Rival Factors

Are U.S. rivals positioned for strategic advantage in this technology?

- Are rivals ahead in this area? Is there a need for an offset/leapfrog move due to blindspots of U.S. commercial investment?
- Are rivals substantially trying to get ahead (strategy, invested, determined, aligned public and private efforts towards its development)?
- Are rivals likely to get ahead due to technology readiness level in their ecosystems compared with the U.S. ecosystem?
- Do rival economic/political systems obviously favor development of this technology over others (e.g. resource allocation, regulatory environment, norms)?
- Does this technology represent a major or potential front along clashing tech-spheres of influence?
- How will U.S. rivals react to U.S. development of or leadership in this technology? Does this technology intersect with weaknesses, organizational inertias, or fundamental asymmetries of U.S. rivals?
- Can we foresee how future rival leadership in this space could fundamentally undercut U.S. leadership and power?

Domestic Factors

What needs to be done to ensure a strong U.S. position?

- Is the U.S. innovation ecosystem naturally generating sufficient advantage?
- Is there a clear U.S. competitive advantage surrounding this technology that needs a national endeavor to harvest?
- What is the maturity level of this technology? Would the U.S. need to “invent the future” to achieve positional advantage?
- Has the U.S. government listed this technology as a priority threat or opportunity area? What is the level of political or social will for this technology?
- Do allies and partners currently possess the key expertise and materials/resources in this technology?
- How might other countries respond to a U.S. national endeavor and are there obvious opportunities for joint efforts with allies?
- Which factors (incentives, financial, political, organizational, or regulatory) are currently limiting progress on this technology in the U.S.? Are these in the USG’s control?

Altogether, this framework provides a template for sorting strategic signals from noise in a time when multiple technologies are advancing and converging, and a rival is determined to overtake the United States as the world's technological powerhouse. Policymakers should not expect a signal to emerge based on specific answers to each question or reaching a certain threshold of particular answers. Rather, the framework sets a process for interrogating technologies to draw out their national significance, potential role in the competition, and the actions for catalyzing advantage. Ultimately, it is the responsibility of policymakers to make judgments by assessing the framework's answers in light of contemporary strategic circumstances.

Studying the Horizon

Unifying public and private actors to fill national technology gaps and seize opportunities requires a systematic approach to scanning the technology horizon.

The capacity to put a stethoscope to the U.S. commercial ecosystem is the prerequisite for developing a technology strategy. As the sources of innovation evolve, the U.S. Government requires new approaches for maintaining awareness of the technologies that can reshape the world. In an international competition with a rival that systematically studies the global technology ecosystem, awareness is the first step in avoiding falling behind in strategic technologies.

In an international competition with a rival that systematically studies the global technology ecosystem, **awareness is the first step** to avoid behind in strategic technologies.

A systematic approach, using the framework outlined above, would empower an entity with a whole-of-nation mandate that sits at the center of a network of horizon scanners, continuously tracking and assessing the technological realm of the possible, the players in the innovation ecosystem, and the potential holes that could have profound impacts.

That network of horizon scanners should include and leverage those incubators and startups that are tackling some of the “toughest tech” but who are outside the traditional government innovation ecosystem.¹¹ Additionally, collaboration with similar entities in partner governments, from Japan to the United Kingdom (UK), India, and Israel, can help

¹¹ See e.g., Katie Rae, [Tough Tech Landscape](#), The Engine (2021).

inform national technology policies.¹²

The necessary elements are already in place. America possesses immense talent in this space – horizon scanning elements already exist everywhere from investment banks and think tanks to universities and venture capital funds.¹³ Folding voluntary private sector experts into an unclassified strategy process that produces “business intelligence” would mark a step change in the U.S. understanding of international rivals.¹⁴

Curating the Platforms of the Future

Achieving national technology goals requires action plans that consider both the technology itself (its maturity, development pathway, and hurdles to viability) and the factors in its broader ecosystem that would enable it to scale, deploy, and commercialize.

Curating a national technology move requires an action plan that facilitates taking a technology from concept to reality. While pure discovery remains crucial, in an international competition leadership derives from national ecosystems that can scale, deploy, and commercialize the technologies with potential to change the world.¹⁵ Action plans seek to nudge loose innovative potential from status quo constraints, whether due to misaligned commercial incentives, regulatory hurdles, talent shortages, or other challenges.

An action plan must see a technology’s role in the market, particularly its commercial purpose and user base. Some technologies, such as hypersonic

While pure discovery remains crucial, in an international competition leadership derives from national ecosystems that can **scale, deploy, and commercialize** the technologies with potential to change the world.

¹² NISTEP Report No. 183, [The 11th Science and Technology Foresight: S&T Foresight 2019: Summary Report](#), National Institute of Science and Technology Policy, Tokyo (2019); [Horizon Scanning Programme Team](#), Government of the United Kingdom (last accessed 2022); [Horizon Scan 2050 A Different View of the Future](#), Stichting Toekomstbeeld der Techniek (2014); [Foundation for the Future of Technology](#), Stichting Toekomstbeeld der Techniek (last accessed 2022).

¹³ Examples of horizon scanning initiatives in government, think tanks, and the private sector include the Department of Homeland Security’s Tech Scouting and Transition Division, the Atlantic Council’s Emergent Futures Lab, and Deutsche Bank’s insights shared in its Horizon Scanning podcast. See [Horizon Scanning](#), Department of Homeland Security (2022); [Emergent Futures Lab](#), Atlantic Council (2018); [Horizon Scanning](#), Deutsche Bank (last accessed 2022).

¹⁴ For other elements on how to address this challenge, see Chapter 6 of this report.

¹⁵ Jeffrey Ding, [The Rise and Fall of Great Technologies and Powers](#) (2021).

weapons, are the exclusive purview of governments and require the state to create and sustain the demand. In other cases, the state need not permanently maintain the market, but only provide a minor nudge, such as the Defense Advanced Research Projects Agency (DARPA)'s 2004 "grand challenge" on autonomous driving that helped spur the current wave of innovation in autonomous vehicles.¹⁶ Thus, an action plan must begin by understanding a technology within its development and commercial context.

An action plan seeks to create a minimum viable solution for realizing a technology on a national scale. Developing such a plan requires two levels of analysis. First, a nation must map the technology pathway¹⁷ for leadership in a specific platform or sector. An action plan's scope and scale depend on the technology's current readiness level.¹⁸ A plan must identify technical hurdles to viability, whether in concept, design, or scaling, before determining the type and level of necessary assistance.

Second, a national action plan must understand an emerging technology's surrounding ecosystem. Here consulting with actors across government, academia, industry, and civil society can help identify what types of government or private interventions could prevent or fill holes in the innovation ecosystem. A comprehensive understanding of the ecosystem also requires mapping factors that are exogenous to the core innovation, but necessary for its full realization, such as public infrastructure, the regulatory environment, the capacity to produce the product at scale, and required resources and supply chains. A full action plan thus marries a technology path to a broader techno-industrial strategy for the ecosystem.

Mobilizing the Entrepreneurs of American Advantage

To best challenge China's fused public-private innovation ecosystem, America requires a more coordinated whole-of-nation effort to energize its own innovation ecosystem toward developing positional advantage in strategically significant technologies.

Recognizing key technologies and building an action plan are necessary steps, but the U.S. ecosystem must actually act. To best compete, the United States must recognize and

¹⁶ This framing outlining four types of markets for technologies is inspired by SCSP's May 2022 engagement with a leading technologist. The four types include: (1) instances where the market functions on its own; (2) instances where the market requires a minor governmental nudge; (3) instances where the market requires substantial (and possibly permanent) governmental engagement; and (4) instances where the private sector recognizes new technological challenges/opportunity of which the government is not aware. See also [The Grand Challenge](#), Defense Advanced Research Projects Agency (last accessed 2022).

¹⁷ These pathways can be charted from a future goal backwards ("back-casting") or via a projection from the current state ("tech trees" or "tech vectors"). See Simon Elias Bibri, [Backcasting in Future Studies: A Synthesized Scholarly and Planning Approach to Strategic Smart Sustainable City Development](#), European Journal of Futures Research at 10-12 (2018); Aaron King & Allison Duettmann, [Growing Tech Trees for Longevity, Molecular Machines, Neurotech, Computing, and Space](#), Foresight Institute (2021).

¹⁸ The concept of "technology readiness levels" was originated by NASA but has become more widely used. See [Technology Readiness Level](#), NASA (2021); [ISC Technology Readiness Level Scale](#), Government of Canada (2020).

work to close holes in its innovation ecosystem, particularly concerning “deep tech,” to fully harness latent potential.¹⁹ Mobilizing a whole-of-economy effort requires matching the power of China’s fused system, but doing so by drawing on American strengths, not mimicking China’s state-centric, authoritarian approach.

Currently, the U.S. innovation ecosystem is under-performing for five reasons:

- *High costs/risks lessen investment in certain strategic technologies.* Recently, high capital costs and risks have prompted firms to avoid certain fields, particularly hardware like semiconductor production,²⁰ that geopolitics have made strategic needs.²¹
- *Certain regulatory hurdles can encumber viable technologies.* Regulation that is outdated, inconsistent across jurisdictions, or inadequately reflective of externalities can hamper the testing, scaling, and commercialization of even proven technology.²²
- *Uncertainty on necessary accompanying innovations or infrastructure can chill investors or limit scalability.* If a component of the ecosystem necessary to support a technology seems implausible or an essential update to public infrastructure seems unlikely, innovation can be stranded.²³
- *Outdated acquisition models deny government leading technologies.* Federal

Mobilizing a whole-of-economy effort requires matching the power of China’s fused system, but doing so by **drawing on American strengths**, not mimicking China’s state-centric, authoritarian approach.

19 “Deep tech” portends a large impact, but requires “a long time to reach market-ready maturity” and significant “capital to develop and scale.” Massimo Portincaso, et al., [Deep Tech Ecosystems](#), Boston Consulting Group (2019).

20 On a growing reluctance to invest in hardware-intensive technology, see Josh Lerner & Ramana Nanda, [Venture Capital’s Role in Financing Innovation: What We Know and How Much We Still Need to Learn](#), Harvard Business School Working Paper Working Paper 20-131 at 9 (2020). Chapter 2 of this report discusses the case of semiconductors in further detail.

21 Julian Kamasa, [Chip Shortages in the Light of Geopolitics and Climate Change](#), Center for Strategic and International Studies (2022); Shane Tews, et al., [The Geopolitical and National Security Implications of Computer Chips: Highlights from a Conversation with Chris Miller](#), AEIdeas (2022).

22 See Travis Brown, [50 States of Chaos: Patchwork Regulation is Crippling Tech Innovation](#), Forbes (2014).

23 For instance, a lack of public investment in the U.S. rail networks have contributed to the minimal development of the U.S. high speed rail sector, particularly compared to international leaders. Natasha Frost, [A Decade Ago, the US was Promised High-speed Rail – So where is it?](#), Quartz (2020); Ben Jones, [Past, Present and Future: The Evolution of China’s Incredible High-speed Rail Network](#), CNN (2022).

acquisition is not geared for purchasing leading commercial technologies, reducing access to new systems. Relationships with legacy industry gatekeepers also crowd out new innovators.²⁴

- *The need for trusted capital flows.* A small subset of capital from select malign foreign actors can distort U.S. markets by facilitating technology transfer or artificially driving up U.S. firms' valuations, interfering in the investment market.²⁵

An enhanced public-private model would overcome these challenges to unlock latent national potential by:

- *Systematically expanding the volume and coordination of information sharing.* Voluntary information sharing cannot only create positive loops between government and the private sector, but also spur greater private-to-private awareness and cooperation.
- *Creating markets in strategic areas.* The Government can help identify strategic technology areas and incentivize private investment and action. Incentives can come in setting moonshots,²⁶ regulatory updates,²⁷ de-risking investment,²⁸ or a targeted technology fund.²⁹
- *Improving government-wide fast-tracks for acquiring new technologies.* Acquisition reform should focus on purchasing for innovation. In a contest of judging how well governance models deliver, America cannot afford to compete with legacy

24 SCSP Platforms Panel Meeting (May 2022). See also Christopher Kirchoff, [Reshaping National Security Institutions for Emerging Technology](#), Aspen Institute at 92 (2016) (paper within America's National Security Architecture).

25 SCSP Platforms Panel Meeting (May 2022). See also Michael Brown & Pavneet Singh, [China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation](#), Defense Innovation Unit Experimental (2018); Sean O'Connor, [How Chinese Companies Facilitate Technology Transfer from the United States](#), U.S.-China Economic and Security Review Commission at 4-7 (2019).

26 Scott Anthony & Mark Johnson, [What a Good Moonshot Is Really For](#), Harvard Business Review (2013); Astro Teller, [Google X Head on Moonshots: 10X Is Easier Than 10 Percent](#), Wired (2013). As a recent example, in 2022 President Biden reinitiated the national cancer moonshot. [Cancer Moonshot](#), National Cancer Institute (2022).

27 James Pethokoukis, [Is Regulation Slowing Tech Progress and Innovation? A Long-read Q&A with Eli Dourado](#), AEIdeas (2016); Larry Downes, [Fewer, Faster, Smarter](#), Democracy (2015); Travis Brown, [50 States Of Chaos: Patchwork Regulation Is Crippling Tech Innovation](#), Forbes (2014).

28 SCSP Platforms Panel Meeting (May 2022). See also Livio Valenti, et al., [Deep Tech Entrepreneurship: From Lab to Impact](#), Belfer Center for Science and International Affairs at 8 (2022); Massimo Portincaso, et al., [The Deep Tech Investment Paradox: A Call to Redesign the Investor Model](#), BCG at 15-16 (2021). Notable current government investment programs include defense-oriented investment entities like the Air Force's AFWERX and the Small Business Administration's Small Business Investment Company program. [About Us](#), AFWERX (last accessed 2022); [SBIC Program Overview](#), Small Business Administration (2018).

29 Such a fund could work as an "OCO for critical technology." On the Overseas Contingency Operations fund (OCO), see Brendan McGarry & Emily Morgenstern, [Overseas Contingency Operations Funding: Background and Status](#), Congressional Research Service (2019).

equipment.

- *Mapping the long-term resource ecosystem.* The U.S. Government and private sector firms can help each other see resource and supply chain risks. Mapping long-term needs avoids the trap of inaccurate predictions.³⁰
- *Certifying trusted capital.* Beyond the Committee on Foreign Investment in the United States (CFIUS), which some investors in early-stage firms have limited exposure to, an information sharing initiative that certifies “trusted capital” could help reduce risks and lower transaction costs for early-stage investors, particularly when acting across different investment communities, by providing an additional reassurance that a promising project did not involve malign foreign capital.
- *Scaling successful models at innovation hubs around the nation.* The nation should learn from and, where appropriate, replicate a new generation of technology incubators focused on “deep tech.”³¹

Together, these lines of effort can further strengthen an already robust American model. They require, however, an organizing force to maximize the chance for successful implementation.

Organizing the Government-Private Sector Nexus

Today’s techno-economic competition demands organizational reform to coordinate a new public-private partnership model and implement the outlined technology strategy process.

The preceding process requires an institutional home to make a new public-private model a reality for sustained long-term technology competition. Ideally, such an entity would serve three core functions: coordinate between public and private stakeholders – and across government actors; provide analytical capacity to inform policymakers; and operate as an action arm, implementing action plans to push strategic technologies forward. Such an entity would also ensure coordination between the action plans and a broader, national

30 SCSP Platforms Panel Meeting (May 2022). See also Willy Shih, [Global Supply Chains in a Post-Pandemic World](#), Harvard Business Review (2020).

31 The U.S. innovation ecosystem is home to a variety of types of technology incubators. An emerging class of incubators that focus on “tough/deep tech” that is often hardware-intensive or possessing a long timeline already are creating results in this area that has received insufficient focus and support. Josh Lerner & Ramana Nanda, [Venture Capital’s Role in Financing Innovation: What We Know and How Much We Still Need to Learn](#), Harvard Business School Working Paper Working Paper 20-131 at 9 (2020). The Engine and the growing Hacking for Defense network reflect two models worthy of further study. See e.g., [Our Mission](#), The Engine (last accessed 2022); [Hacking for Defense](#), H4D (last accessed 2022).

techno-industrial strategy.³² Several options merit consideration.

The executive branch could elect to create a technology competitiveness hub by executive order. As the case of the National Economic Council (NEC) illustrates, presidents have taken it upon themselves to create new organizational capacities to meet changing global circumstances.³³ Similarly today, the President could determine that international competition requires a focal point in the executive branch that could support senior leadership engagement with the private sector, the coordination of information flows for presidential-level decisions, and accountable implementation of a technology strategy process.

Alternatively, a technology competitiveness hub could be deemed essential and relevant legislation could be passed establishing an office(s) in the executive or legislative branches. The National Security Council (NSC), today a principal tool for the President within the Executive Office of the President, was mandated by legislation.³⁴ A legislative grounding helps ensure an entity's staying power when compared to functions created at the President's discretion, reducing its exposure to political whim. Currently, legislative proposals for a Technology Competitiveness Council (TCC) and an Office of Global Competition Analysis (OCA) are under consideration and are worthy of study.³⁵ A legislative branch agency, like the Congressional Research Service,³⁶ or a federally funded research and development center (FFRDC),³⁷ could fulfill many of the analytical functions, as well as the information-sharing dimension of coordination. However, a legislative branch agency or FFRDC would

³² For more on techno-industrial strategy, see Chapter 2 of this report.

³³ Executive Order 12835, [Establishment of the National Economic Council](#), The American Presidency Project (1993). The NEC responded to changing international conditions as it sought to unite "international and economic policy" in a single forum. Sarah Rosen Wartell, [National Economic Council](#), Change for America at 16 (2008).

³⁴ Pub. L. 80-253, [The National Security Act of 1947](#) (1947); Kathleen McInnis & John Rollins, [The National Security Council: Background and Issues for Congress](#), Congressional Research Service at 5-7 (2021).

³⁵ In 2022, Congress considered legislation for both a Technology Competitiveness Council (TCC) and Office of Global Competition Analysis (OCA). H.R. 8027, [To Establish within the Executive Office of the President a Technology Competitiveness Council](#) (2022); Courtney Albon, [Lawmakers Propose 'Technology Competitiveness Council' to Champion US Innovation](#), C4ISRNet (2022); S. 4368, [American Technology Leadership Act of 2022](#) (2022); Daniel Flatley, [Senators Wary of China's Tech Prowess Seek Competition Office](#), Bloomberg (2022). The NSCAI recommended creating a TCC in its final report in 2021. [Final Report](#), National Security Commission on Artificial Intelligence at 166 (2021). A combination of a TCC and an OCA could be a powerful duo in advancing U.S. organizational capacity to compete. OCA – housed in the Executive Office of the President, an executive agency, or an FFRDC – could provide analytical capacity for senior policymakers while remaining insulated from the momentary political pressures and ensuring intellectual memory across administrations. Complementary, a TCC located in the White House would offer both a key point of engagement between governmental leaders and the private sector and an action arm for pursuing action plans and moving the national innovation ecosystem.

³⁶ The Congressional Research Service is an example of a legislative branch agency established by statute but situated in the legislative branch to provide research and analysis. See Ida Brudnik, [The Congressional Research Service and the American Legislative Process](#), Congressional Research Service (2011).

³⁷ See Marcy Gallo, [Federally Funded Research and Development Centers \(FFRDCs\): Background and Issues for Congress](#), Congressional Research Service at 4 (2021).

be more limited in its ability to implement policy, which is a function of the executive branch.

Finally, should governmental action be stymied, a public-private partnership could pick up the torch to provide analysis and serve as a convening center for information sharing. Though also limited in its capacity for implementation, a nongovernmental entity, including an FFRDC,³⁸ could offer advantages of independent research and analysis, intellectual consistency across administrations, and “neutral ground” that fosters access to government without being “of government.”

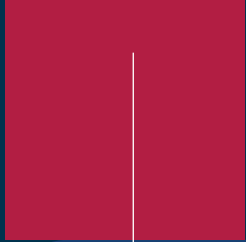
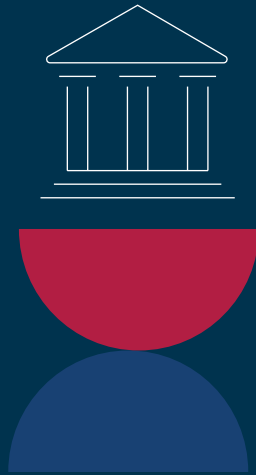
Ultimately, the three preceding approaches are not mutually exclusive. The American innovation ecosystem is a complex and multifaceted domain. It brings together a host of actors — from innovators and academics to investors, regulators, and the crowd. So too might a successful organizational paradigm draw on the executive branch, legislative branch, FFRDCs, and new public-private organizations to best align the nation to compete.

38 While Congress could create an FFRDC by legislation, legislation is not necessary to create a new FFRDC. The “Federal Acquisition Regulation system (FAR) governs the establishment, use, review, and termination of FFRDCs.” Marcy Gallo, [Federally Funded Research and Development Centers \(FFRDCs\): Background and Issues for Congress](#), Congressional Research Service at 4 (2021).

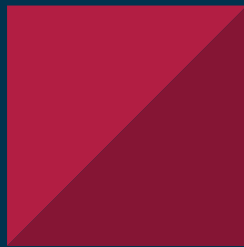
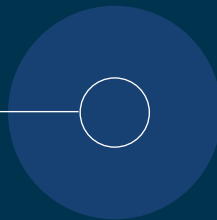
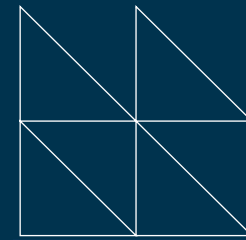
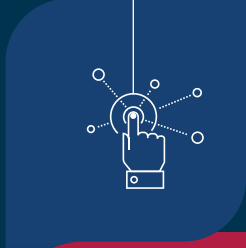
Restoring the Sources of Techno- Economic Advantage

Mid-Decade Challenges to National Competitiveness

02



- **Toward a Techno-Industrial Strategy**
- **Pipes: Digital Infrastructure for a Next-Generation Economy**
- **People: Winning the Global Competition for Talent**
- **Production: Securing Access to Critical Technology Inputs**
- **Preserve: U.S. Financial Leadership in the Digital Age**
- **Pushback: Coercive Economic Statecraft**



CHAPTER 2

Restoring the Sources of Techno-Economic Advantage

Strong economic foundations enable societies to thrive and provide the resources for nations to sustain technology leadership, craft a competitive foreign policy, and project military power. While the United States holds the upper hand across a number of economic fundamentals,¹ China's techno-economic advance is testing whether America can continue to translate its advantages into national power without changing course. The PRC's economic size, second only to the United States in market terms,² and ability to project economic power globally make it an unprecedented rival — larger and more powerful than the Soviet Union during the Cold War. Beijing has put the coercive power of the state at the forefront of its economic strategy, claiming that its Leninist, single-party dictatorship is better equipped than democracies to invent the future.³ Massive government support for domestic industry, coupled with rampant technology theft abroad and other unfair policies, have wiped out jobs, companies,

1 Economic fundamentals can be framed in terms of key inputs or factors of production. These typically include land (i.e., natural resources), labor, and capital. Innovation, also known as total factor productivity, determines how productively these inputs are combined. SCSP assesses that the United States is better off than China on land (as a net exporter of energy and agriculture; China is a net importer of both), labor (the U.S. workforce is highly productive and growing, while China's is less productive and shrinking), and innovation. On capital, China is moving faster to accumulate physical capital (infrastructure and factories), while the United States has a strong lead in finance, which offers advantages for productive investments. SCSP's assessment was informed by *Welcome to the Machine: A Comparative Assessment of the USA and China to 2035 Focusing on the Role of Technology in the Economy*, Fathom Financial Consulting Limited (2022) (*SCSP-commissioned work product*).

2 *Welcome to the Machine: A Comparative Assessment of the USA and China to 2035 Focusing on the Role of Technology in the Economy*, Fathom Financial Consulting Limited (2022) (*SCSP-commissioned work product*).

3 Beijing self-identifies as a Marxist-Leninist dictatorship and says that features of this system are essential to China's success, including a "scientific" assessment of world trends in which China is ascendent and western capitalism is in decline; a campaign-style approach to using people and resources to achieve national objectives; and long-term planning. Dan Tobin, [How Xi Jinping's New Era Should Have Ended U.S. Debate on Beijing's Ambitions](#), Center for Strategic and International Studies (2020). For a thoroughly-researched, book-length treatment of the PRC's grand strategy, see Rush Doshi, [The Long Game: China's Grand Strategy to Displace American Order](#), Oxford University Press (2021).

Beijing has put the coercive power of the state at the forefront of its economic strategy, claiming that its Leninist, single-party dictatorship is better equipped than democracies to invent the future.

and entire industries and suppressed innovation in advanced economies.⁴

The economic competition is America's to lose. The United States holds massive advantages, including the world's largest and most liquid financial markets, the dollar's status as the global reserve currency, and a diversified and resilient economy that has a strong track record of bouncing back from downturns. Additionally, a world-class innovation ecosystem, a highly

productive labor force, the ability to attract global talent, and trusted legal and regulatory institutions make the United States the world's most dynamic economy.⁵ More than any other nation, American capital builds prosperity around the world in the form of foreign direct investment (FDI).⁶ America can significantly amplify its advantages by working with allies, as democracies account for more than 60 percent of the world's gross domestic product (GDP).⁷

But there are storm clouds on the horizon. The United States is falling behind in advanced industries, including high-capacity batteries and microelectronics.⁸ Decades of hands-off economic policies have accelerated the outsourcing of American manufacturing to East Asia.⁹ The U.S. technology sector, left on its own and driven by short-term imperatives to reduce labor and capital expense, has skewed heavily towards software and services, leaving America with critical vulnerabilities in hardware production.¹⁰ The United States

4 See Stephen Ezell, [False Promises II: The Continuing Gap Between China's WTO Commitments and Its Practices](#), Information Technology & Innovation Foundation (2021); Robert D. Atkinson, [Innovation Drag: China's Economic Impact on Developed Nations](#), Information Technology & Innovation Foundation (2020).

5 Klaus Schwab, [The Global Competitiveness Report 2018](#), World Economic Forum at 33-34 (2018).

6 The U.S. has more than \$6 trillion in outward FDI stocks, see [Direct Investment by Country and Industry](#), U.S. Bureau of Economic Analysis (2022). The second-largest source of FDI, the PRC, has a total stock of outward FDI of approximately \$2 trillion, see [U.S.-China Investment Ties: Overview](#), Congressional Research Service (2021).

7 Tom Orlick, et al., [A Third of the Global GDP is Now Generated by Non-Democracies](#), Bloomberg (2022).

8 Richard Florida, [Advanced Industries Still Rule the U.S. Economy—But It's an Advantage That's Slipping](#), Bloomberg (2015); [FACT SHEET: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities](#), The White House (2021).

9 Matthew C. Klein, [The American Dream: Bringing Factories Back to the U.S.](#), Barron's (2020); Robinson Meyer, [The Bill That Could Truly, Actually Bring Back U.S. Manufacturing](#), The Atlantic (2021).

10 Between 1979 and 2019, the U.S. lost 6.7 million total manufacturing jobs. See Katelynn Harris, [Forty Years of Falling Manufacturing](#)

now finds itself unable to manufacture critical goods that it needs, and brittle supply chains leave the country vulnerable to supply shocks.¹¹

The United States must respond by crafting a Techno-Industrial Strategy (TIS)¹²— an industrial strategy focused on cutting-edge technology sectors that drive economic growth and are critical for national security. A Techno-Industrial Strategy should build on America’s fundamental strengths to boost economic output and fill national security gaps, yielding spillover benefits for the entire economy.¹³ Though some maintain that industrial strategy is inefficient, harmful, and runs counter to free market principles,¹⁴ targeted intervention can generate wealth and fill gaps when the market falls short.¹⁵ A TIS should focus on two objectives:

- *Encourage Technology Diffusion.* To stay ahead, the United States must scale emerging technologies like microelectronics, 5G, and AI more quickly. Moving technologies from the lab to the market boosts economic output, creating national wealth and improving livelihoods. Economists recognize a role for the government in funding research and development (R&D) and scaling emerging technologies through workforce and infrastructure investment — areas where the market tends to fall short.¹⁶

A Techno-Industrial Strategy should build on America’s fundamental strengths to boost economic output and fill national security gaps, yielding spillover benefits for the entire economy.

[Employment](#), U.S. Bureau of Labor Statistics (2020).

11 [Remarks on a Modern American Industrial Strategy By NEC Director Brian Deese](#), The White House (2022).

12 SCSP has coined this term to refer to the approach proposed in this paper. It includes traditional elements of industrial strategy as commonly understood by economists, i.e. government intervention to stoke innovation and strengthen sectors considered essential for economic and national security, as well as other elements that are important to the competition with China, as laid out in the Preserve and Pushback sections of this chapter.

13 Mariana Mazzucato, et al., [Industrial Policy’s Comeback](#), Boston Review (2021); Gregory Tasse, [The Economic Rationales and Impacts of Technology-Based Economic Development Policies](#), Economic Policy Research Center at 1-8 (2018).

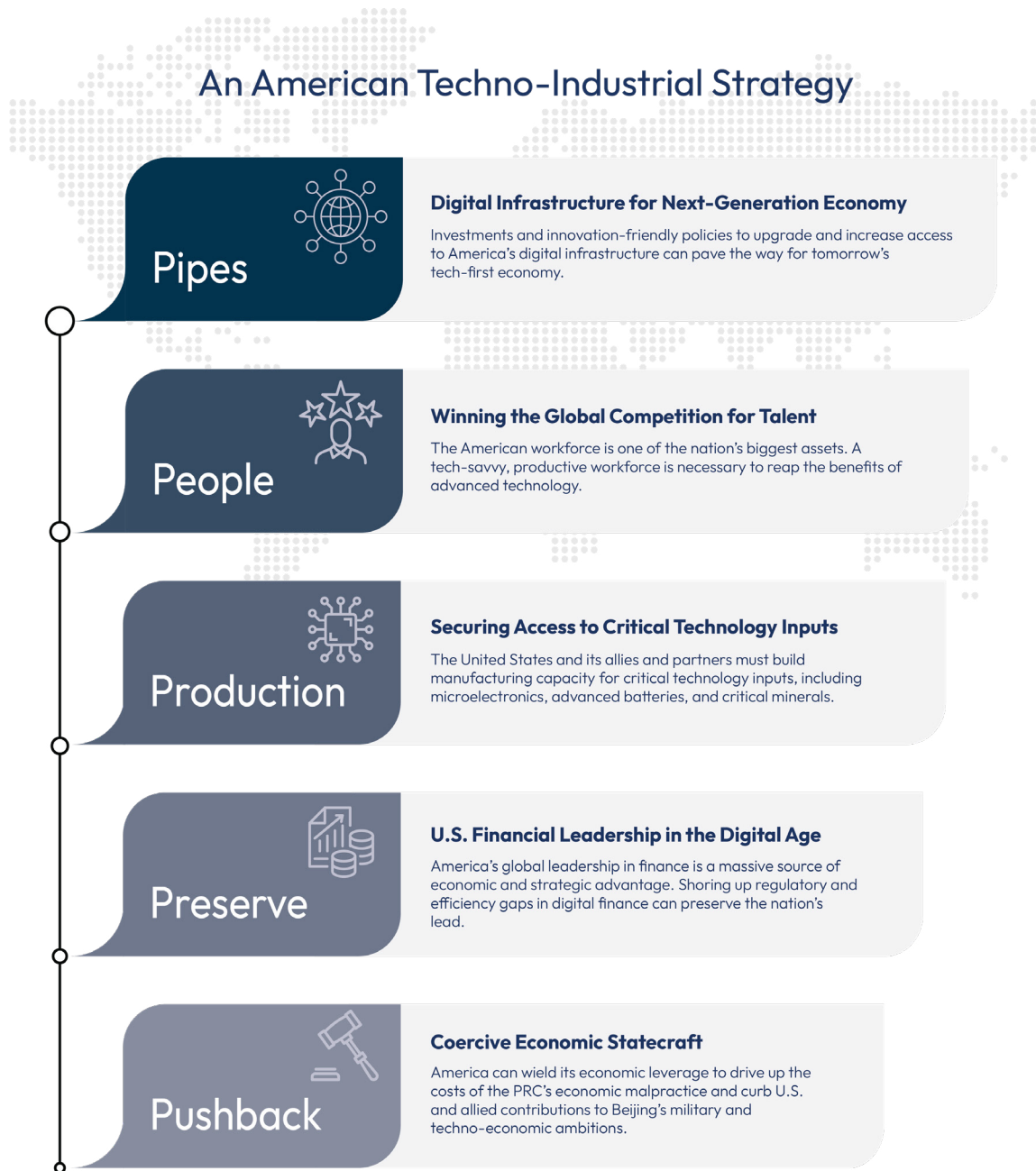
14 Charles Schultze, [Industrial Policy: A Dissent](#), The Brookings Review (1983); Scott Lincicome & Huan Zhu, [Questioning Industrial Policy: Why Government Manufacturing Plans Are Ineffective and Unnecessary](#), Cato Institute (2021).

15 Marc Fasteau & Ian Fletcher, [The Economic Foundations of Industrial Policy](#), Palladium (2020).

16 Markets often fail to account for the massive economic benefits that accrue from spending on R&D, infrastructure, and workforce training, and infrastructure. See, e.g., Timothy F. Bresnahan & Manuel Trajtenberg, [General Purpose Technologies: “Engines of Growth?”](#), National Bureau of Economic Research at 18-21 (1992). On the benefits of government policies to boost R&D, see [Welcome to the Machine: A Comparative Assessment of the USA and China to 2035 Focusing on the Role of Technology in the Economy](#), Fathom Financial Consulting

- *Fill Economic and National Security Gaps.* Running faster will not be enough to stay ahead. The United States must close critical supply chain vulnerabilities, preserve global financial leadership, and ensure that its technological innovations and capital do not fuel PRC military capabilities or techno-economic malpractice.

A TIS must include the following lines of effort:



Toward a Techno-Industrial Strategy

Industrial strategy is part of the American experience. Throughout its history, the U.S. Government has responded to times of strategic competition and national emergency by partnering with the private sector to correct market failures and fill critical technology gaps.¹⁷ In recent decades, policymakers have overlooked America’s history of leveraging public-private partnerships to push the technological frontier and promote diffusion. Today, however, industrial strategy is enjoying a resurgence. The White House has called for a “Modern American Industrial Strategy,”¹⁸ and President Biden signed into law the CHIPS and Science Act, a \$280 billion spending package to revive American innovation that includes \$52 billion for semiconductor production and research.¹⁹ Washington should build on this traction by providing incentives and making investments in strategic technologies to ensure America remains ahead, drawing on lessons from the past.

The United States has a long history of employing industrial strategies to boost national advantage. In 1791, Treasury Secretary Alexander Hamilton submitted his *Report on the Subject of Manufactures* to Congress proposing a slate of measures to support manufacturing in strategic industries.²⁰ Hamilton’s vision was realized a few decades later under the American System, an industrial strategy that included subsidies to build railroads, canals, armories, and other forms of infrastructure.²¹ Abraham Lincoln advanced this strategy by signing legislation that chartered the Transcontinental Railroad and established a system of land grant colleges.²² By the early 20th century, the United States had emerged as a global power. Industrial strategy projects – including World War II mobilization and Cold War-era government interventions that jump-started the microelectronics industry – strengthened the country’s techno-economic foundation, readying it for strategic rivalries with Germany, Japan, and later with the Soviet Union.²³

Well-crafted industrial strategies encourage – not stifle – competition among firms. Establishing market conditions is the best way for the government to foster competition.

17 Martijn Rasser, et al., [Reboot: Framework for a New American Industrial Policy](#), Center for a New American Security (2022); Walter M. Hudson, [Geoeconomic Strategy and National Developmentalism](#), National Development (2022).

18 [Remarks on a Modern American Industrial Strategy By NEC Director Brian Deese](#), The White House (2022).

19 Pub. L. 117-167, [The CHIPS and Science Act of 2022](#) (2022).

20 Alexander Hamilton, [Final Version of the Report on the Subject of Manufactures](#), U.S. Department of the Treasury (1791).

21 Maurice Baxter, [Henry Clay and the American System](#), University Press of Kentucky at 49-54 (1995).

22 Michael Lind, [Land of Promise: An Economic History of the United States](#), Harper at 152-153 (2012); [Land-Grant College Act of 1862](#), Encyclopedia Britannica (last accessed 2022).

23 Arthur Herman, [Freedom’s Forge: How American Business Produced Victory in World War II](#), Random House at 192-200 (2012); Charles A. Murray & Catherine Bly Cox, [Apollo: The Race to the Moon](#), Simon & Schuster at 25 (1989).

Opponents frame industrial strategy as the government’s attempts to “pick winners.”²⁴ However, successful industrial strategies can create market conditions that do not naturally exist, allowing firms to compete to meet the national demand.²⁵ The government can jump-start markets by setting high technical “bars,” accompanied by results-oriented metrics, and rewarding entrepreneurs who meet them.²⁶ Operation Warp Speed, a public-private partnership initiated by the White House, followed this template and fielded COVID-19 vaccines in a record 10 months.²⁷

Pipes: Digital Infrastructure for a Next-Generation Economy

Technologies driving 21st-century economic growth, like artificial intelligence, rely on digital infrastructure — including 5G networks, satellite arrays, and IoT devices — to connect and power them. The United States can pave the way for an AI-driven society and economy through swift investment in secure domestic digital infrastructure, removing regulatory hurdles, and forming public-private partnerships to foster private sector-driven innovation. Ensuring rapid diffusion of digital technologies will promote broad-based growth and offer secure, speedy links to all Americans.

*The United States should move quickly to build out secure digital infrastructure for broadband access, 5G networks, satellite arrays, and IoT edge devices to reach businesses and citizens across America. With tens of billions of dollars already appropriated for a nationwide broadband rollout, the focus now must be on rapid, maximum-impact execution, optimizing for both network security and procurement cost.*²⁸ The Federal Communications Commission should set more ambitious deadlines and adequately fund federal requirements for telecoms and Internet service providers to implement “Rip and Replace” rules to remove PRC-made Huawei and ZTE components.²⁹

U.S. authorities should implement policies to expand public and private 5G network reach. Wired optical networks will underpin digital connectivity, but the development of 5G and 6G fixed-wireless access, low-Earth-orbit satellites, and other technologies can offer

24 Chiara Criscuolo, et al., [Are Industrial Policy Instruments Effective?](#), OECD at 24-28 (2022).

25 In the context of national policy, this can occur as part of the technology action plans described in Chapter 1 of this report.

26 Philippe Aghion, et al., [Industrial Policy and Competition](#), American Economic Journal: Macroeconomics at 17-23 (2015).

27 The program set a “stretch goal” – rapid vaccine development and deployment – and used bar-setting criteria to select three promising vaccine technology platforms. Then, it baked competition into the program by selecting two companies per platform. See Moncef Slaoui & Matthew Hepburn, [Developing Safe and Effective Covid Vaccines – Operation Warp Speed’s Strategy and Approach](#), New England Journal of Medicine (2020).

28 GAO-22-104611, [National Strategy Needed to Guide Federal Efforts to Reduce Digital Divide](#), U.S. Government Accountability Office (2022); Robert D. Atkinson, [How Applying ‘Buy America’ Provisions to IT Undermines Infrastructure Goals](#), Information Technology & Innovation Fund (2022).

29 John Hendel, [Why Suspected Chinese Spy Gear Remains in America’s Telecom Networks](#), Politico (2022).

competitive alternatives for last-mile broadband, especially in underserved communities. The U.S. Government should make more radio spectrum available to commercial users — not only for telecom networks, but also for smaller firms and private 5G networks and Open Radio Access Network (O-RAN) testbeds — and improve the spectrum allocation process.³⁰

The U.S. Government should accelerate R&D and remove barriers for distributed innovation of commercial 5G applications, industrial testbeds, smart cities technologies, and O-RAN architectures, setting out a bold strategy for a “smart society.” 5G cellular networks promise to unlock commercial and public sector applications in smart manufacturing, smart cities, and other uses foundational to the next generation economy.³¹ While PRC firms Huawei and ZTE surged ahead of U.S. competitors in developing and deploying certain 5G network technologies and components,³² no single firm or country has won the still-ongoing race to develop new 5G applications, many of which are yet to be developed.³³ Government should partner with the private sector and create sandboxes to drive development and testing of these applications so America becomes a market leader and standards-setter for 5G applications.³⁴ U.S. authorities should incentivize and fast-track development and deployment of flexible O-RAN and virtualized network architectures, which can create opportunities for more U.S. tech firms, lead to lower network costs, and foster U.S. leadership in international standards setting.³⁵

...no single firm or country has won the still-ongoing race to **develop new 5G applications**, many of which are yet to be developed.

The United States should forge a national data strategy to leverage, securely, America’s data as an asset for its innovators. The initiative should foster responsible artificial intelligence applications while protecting digital privacy and security. A U.S. data strategy should aim to serve citizens, boost economic growth, and provide a model of democratic, innovation-

30 Nihal Krishan, [FCC and NTIA Overhaul Spectrum Coordination Agreement](#), FedScoop (2022).

31 [Accelerating 5G in the US](#), Center for Strategic and International Studies (2021).

32 Steven Levy, [Huawei, 5G, and the Man Who Conquered the Noise](#), Wired (2020).

33 [Patenting Activity Among 5G Technology Developers](#), U.S. Patent and Trademark Office at 1, 9 (2022).

34 [ITI’s 5G Policy Principles and 5G Essentials for Global Policymakers](#), Information Technology Industry Council at 4 (2020).

35 Naima Hoque Essing, et al., [The Next-Generation Radio Access Network: Open and Virtualized RANs Are the Future of Mobile Networks](#), Deloitte (2020).

friendly data governance. The strategy should articulate clear, consistent personal data privacy rights and plan how best to harness data to spur private sector-driven innovation and growth, including responsible AI development. The federal government should make data and cloud computing available to small firms as well as academic researchers and non-profit organizations via a National Research Cloud.³⁶ Creating a clear strategic and regulatory framework for data can offer a positive template for other countries, which currently may look to either China or the EU for models, and lay the groundwork for increased international digital trade and trade agreements based on responsible, open Internet norms.

*The U.S. Government should invest in and integrate cybersecurity measures throughout the nation's digital infrastructure in partnership with private sector and non-profit partners. Authorities should collaborate with technology firms to identify and neutralize threats and vulnerabilities swiftly.*³⁷ One area deserving new focus is the need to address vulnerabilities in non-proprietary open source software and hardware, which are both expanding.³⁸ A way for the government to address such vulnerabilities could be for Congress to authorize the creation of a Center for Open Source Technology Security to identify and catalog technology in need of support and fund critical improvements.³⁹

People: Winning the Global Competition for Talent

Developing, scaling, and adopting emerging technologies – and reaping their economic benefits – requires a productive and tech-savvy workforce.⁴⁰ Today, however, the United States is not producing or recruiting the technical talent it needs.⁴¹ Although interest in emerging technology fields has skyrocketed, the U.S. education and immigration systems are struggling to meet demand.⁴² Nearly one-third of American adults have limited or no

36 See [Final Report](#), National Security Commission on Artificial Intelligence at 191 (2021); see also Daniel Ho, et al., [Building a National Research Resource: A Blueprint for a National Research Cloud](#), Stanford Institute for Human-Centered AI (2021).

37 [Cyberspace Solarium Commission Report](#), U.S. Cyberspace Solarium Commission at 75 (2020).

38 Jason Perlow, [A Summary of Census II: Open Source Software Application Libraries the World Depends On](#), The Linux Foundation (2022).

39 Eric Schmidt & Frank Long, [Protect Open Source Software](#), Wall Street Journal (2022); Ashwin Ramaswami, [Securing Open Source Software at the Source](#), Plaintext by Schmidt Futures (2021). While these assessments recommend centers for Open Source Software (OSS), the growth of open source hardware creates new opportunities and vulnerabilities that should be addressed as part of an Open Source Technology Center encompassing both hardware and software. See Ann Steffora Mutschler, [Open Source Hardware Risks](#), Semiconductor Engineering (2020).

40 Jeffrey Ding, [The Rise and Fall of Great Technologies and Powers](#) (2022).

41 Stephen Ezell, [Assessing the State of Digital Skills in the U.S. Economy](#), Information Technology & Innovation Foundation (2021).

42 Remco Zwetsloot & Jack Corrigan, [AI Faculty Shortages: Are U.S. Universities Meeting the Growing Demand for AI Skills?](#), Center for Security and Emerging Technology at 5-8 (2022); Stephanie Yang, [Chip Makers Contend for Talent as Industry Faces Labor Shortage](#), The Wall Street Journal (2022).

Congress and the Executive Branch must take bold action to advance effective **education, immigration, and workforce development policies.**

digital skills.⁴³ These gaps pose a major threat to U.S. economic competitiveness and national security. In partnership with the private sector and academia, Congress and the Executive Branch must take bold action to advance effective education, immigration, and workforce development policies.

- **Education**

The federal government must heavily invest in STEM and emerging technology education. The NSCAI recommended

a National Defense Education Act (NDEA) II and a U.S. Digital Service Academy (USDSA).⁴⁴ Modeled on the original post-Sputnik legislation, NDEA II would provide landmark investments for students focused on acquiring digital skills, including computer science, data science, information science, mathematics, and statistics. USDSA would be an accredited, degree-granting university that produces government civilians with digital expertise to serve across the U.S. Government's departments and agencies.⁴⁵ The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 proposes a Department of Defense (DoD) Cyber and Digital Service Academy Scholarship.⁴⁶ To address the broader talent shortage, America will need an established academy, and a concerted national effort with education, to provide the scale needed to help close the tech talent gap in government. Current scholarships and programs cannot match the growing demand for talent in government agencies, meaning bold action is required.

The federal government should expand partnerships between industry and academia and leverage apprenticeship programs to train, reskill, and upskill the next generation of emerging technology talent. Developing a tech-savvy workforce will require utilizing and retraining current tech talent to develop cutting-edge programs in universities and community colleges.⁴⁷ Building on the workforce

43 Amanda Bergson-Shilcock, [The New Landscape of Digital Literacy](#), National Skills Coalition at 4 (2020).

44 [Final Report](#), National Security Commission on Artificial Intelligence at 175 (2021).

45 [Final Report](#), National Security Commission on Artificial Intelligence at 368-372 (2021).

46 S. 4543, [James M. Inhofe National Defense Authorization Act for Fiscal Year 2023](#), § 1111, (2022).

47 In 2022, Purdue University unveiled the nation's first comprehensive Semiconductor Degrees Program for graduates and undergraduates, in partnership with various microelectronics firms. [Purdue Launches Nation's First Comprehensive Semiconductor](#)

development provisions in the CHIPS and Science Act of 2022, federal and state governments should incentivize universities and colleges, and tech companies, to educate the future workforce in critical fields and scale existing programs.⁴⁸ In addition, the federal and state governments could expand and tailor tax incentives offered to firms for worker training and apprenticeship programs in strategic industries like semiconductor packaging and battery assembly. These programs can be more cost-effective for companies compared to tuition assistance for workers.⁴⁹

- **Immigration**

The U.S. Government should accelerate immigration processes, increase efforts to attract international tech talent, and target visas directly to needed tech fields. Highly-skilled immigrants have a disproportionately positive impact on innovation and job creation.⁵⁰ In AI and other emerging fields, the United States is competing for a limited pool of talent spread around the world. Proposals such as the Million Talents Program⁵¹ to attract and retain one million “tech superstars” are examples of the bold action America needs to take. The United States should fast-track green cards and visas for workers in strategic sectors and create a separate, targeted “Innovator” visa category.⁵²

The United States should ensure it remains a magnet for tech talent from the PRC and elsewhere, while implementing common sense precautions to protect national security. Students from the PRC and elsewhere with legitimate purposes for coming to the United States should continue to be welcomed. The Department of State should continue to filter out applicants with demonstrated national security risk factors, such as affiliation with the People’s Liberation Army, the PRC’s military-civil fusion (MCF) strategy,⁵³ or talent programs, such as the Thousand Talents

[Degrees Program](#), Purdue University (2022).

48 See e.g., Diana Gehlhaus & Luke Koslosky, [Training Tomorrow’s AI Workforce: The Latent Potential of Community and Technical Colleges](#), Center for Security and Emerging Technology at 29-32 (2022).

49 [Building Strong and Inclusive Economies through Apprenticeship](#), New America, Center on Education & Skills at New America (2019); [Investments, Tax Credits, and Tuition Support](#), U.S. Department of Labor (last accessed 2022).

50 [Entrepreneurship](#), New American Economy (last accessed 2022); John Lettieri & Kenan Fikri, [The Case for Economic Dynamism and Why it Matters for the American Worker](#), Economic Innovation Group (2022).

51 Graham Allison & Eric Schmidt, [The U.S. Needs a Million Talents Program to Retain Technology Leadership](#), Foreign Policy (2022).

52 [Global Talent Visa Program](#), Australian Government Department of Home Affairs (last accessed 2022); [High Potential Individual \(HPI\) Visa](#), UK Government (last accessed 2022).

53 [Military-Civil Fusion and the People’s Republic of China](#), U.S. Department of State (2020).

Plan, known to be CCP conduits for illicit tech transfer.⁵⁴ Despite criticism that such safeguards cost the United States significant tech talent,⁵⁵ the most prominent such policy – the 2020 Presidential Proclamation suspending entry for some students and researchers connected to MCF – has affected a very small minority of PRC student visa applicants.⁵⁶

Strengthen research security. To balance the benefits of international collaboration with the need to protect sensitive intellectual capital from foreign threats, universities and research institutions should develop systems that require disclosure of potential conflicts of interest of researchers and funding organizations.⁵⁷

- **Workforce & Automation**

The United States should invest in automation, as well as training for workers impacted by these technologies, to boost productivity and improve job quality. America should pursue productivity-boosting automation applications. Targeted investments and training can help to mitigate potential displacement and encourage technologies that support American workers. Automation can augment America's workforce, enabling workers to acquire new skills and shift away from dangerous, unsanitary, or repetitive tasks.⁵⁸

Production: Securing Access to Critical Technology Inputs

A techno-industrial strategy must also address gaps that pose strategic-level risks to economic and national security. Over the past several decades, policies based on market fundamentalism – the belief that unrestricted free trade and minimal government intervention is always the best policy – have incentivized companies to offshore critical manufacturing, resulting in an imbalanced U.S. economy with advantages in software. But critical vulnerabilities in hardware leave the nation exposed to supply shocks.⁵⁹ The United

54 Alex Joske, [The Chinese Communist Party's Global Search for Technology and Talent](#), Australian Strategic Policy Institute (2020); Jordan Robertson, [China's Suspected IP Thieves Targeted by Twins' Utah Startup](#), Bloomberg (2022).

55 Stuart Anderson, [Biden Keeps Costly Trump Visa Policy Denying Chinese Grad Students](#), Forbes (2021).

56 See [Proclamation Suspending Entry of Chinese Students and Researchers Connected to PRC "Military-Civil Fusion Strategy"](#), NAFSA (2020). According to the State Department, only about one percent of PRC student visa applicants were affected. See Sha Hua, et al., [Chinese Student Visas Tumble from Prepandemic Levels](#), Wall Street Journal (2022).

57 The University of California has developed a set of best practices and offers training to others. See Elisa Smith, [Research Security Symposium Focuses on Protecting America's Intellectual Capital](#), University of California (2021).

58 Erik Brynjolfsson, [The Turing Trap: The Promise & Peril of Human-Like Artificial Intelligence](#), Daedalus (2022).

59 D. Joseph Stiglitz, [Moving Beyond Market Fundamentalism to a More Balanced Economy](#), Annals of Public and Cooperative Economics at 345-351 (2009); Robert D. Atkinson, [The Hamilton Index: Assessing National Performance in the Competition for Advanced Industries](#), Information Technology & Innovation Foundation (2022); [Remarks on a Modern American Industrial Strategy By NEC Director Brian Deese](#), The White House (2022).

States can fill these gaps, but only if the government is willing to shoulder more of the risk.

The U.S. Government must work with the private sector, and with its allies and partners, to build production capacity for critical inputs to dual-use technologies. The United States should prioritize securing supply of the following high-risk inputs:

- **Rare Earth Minerals & Permanent Magnets:** China controls about 85 percent of rare earth processing.⁶⁰ The PRC has threatened to cut off America's supply of rare earths, which are used in everything from iPhones to jet fighters (a single F-35 requires over 900 pounds of rare earths).⁶¹ Rare earth permanent magnets are used to build green technologies and precision-guided munitions.⁶²
- **Advanced High-Capacity Batteries:** America relies on the PRC for green technologies, including advanced batteries that power electric vehicles and store clean energy.⁶³ China controls about 80 percent of battery production.⁶⁴
- **Microelectronics:** Semiconductors are the brains of modern technology. 100 percent of advanced chips are produced in Asia, leaving the U.S. supply vulnerable.⁶⁵

Each of the industries listed above is critical to U.S. economic and national security, but all stand at risk of supply shocks due to military crises, public health emergencies, natural disasters, or other contingencies. We selected them based on four criteria: **dual-use status**,⁶⁶ **steep barriers to entry**,⁶⁷ **economic importance**,⁶⁸ and **adversary dependence**.

60 Keith Zhai, [China Set to Create New State-Owned Rare-Earths Giant](#), Wall Street Journal (2021).

61 Valerie Bailey Grasso, [Rare Earth Elements in National Defense: Background, Oversight Issues, and Options for Congress](#), Congressional Research Service at 4 (2013).

62 Russell Parman, [An Elemental Issue](#), U.S. Army (2019).

63 Martin Placek, [Share of the Global Lithium-Ion Battery Manufacturing Capacity in 2021 with a Forecast for 2025, by Country](#), Statista (2022); Govind Bhutada, [Mapped: EV Battery Manufacturing Capacity, by Region](#), Visual Capitalist (2022); [Global Gigafactory Pipeline Hits 300: the PRC Dominates but the West Gathers Pace](#), Benchmark Mineral Intelligence (2022).

64 [U.S. Narrows Gap With China in Race to Dominate Battery Value Chain](#), Bloomberg NEF (2021).

65 Antonio Varas, et al., [Strengthening the Global Semiconductor Value Chain in an Uncertain Era](#), Boston Consulting Group & Semiconductor Industry Association at 5 (2021).

66 Rare earths, batteries, and microelectronics each power emerging technologies with a variety of commercial and defense applications. The Department of Defense has identified each of the above inputs as a critical vulnerability. [Securing Defense-Critical Supply Chains: An Action Plan Developed in Response to President Biden's Executive Order 14017](#), U.S. Department of Defense at 1-7 (2022).

67 Entrepreneurs and investors face steep barriers to entry in these sectors, including high capital expenditures, regulatory hurdles, supply chain complexity, and insufficient domestic industrial know-how. See Chris Power, et al., [Rockets, Jets, and Chips: How to Modernize U.S. Manufacturing](#), Future (2022); John VerWey, [No Permits, No Fabs: The Importance of Regulatory Reform for Semiconductor Manufacturing](#), Center for Security and Emerging Technology at 17-24 (2021); Yifei Huang, [Software Is the Tech You Date, But Hardware Is the Tech You Marry](#), London Business School Private Equity & Venture Capital Blog (2022).

68 As of 2014, rare earth production supported about \$300 billion in downstream economic activity. Ann Norman, et al., [Critical Minerals: Rare Earths and the U.S. Economy](#), National Center for Policy Analysis at 3 (2014). The market for lithium-ion batteries alone is poised to reach \$180 billion by 2030. [Lithium-ion Battery Market Size Worth \\$182.53 Billion By 2030: Grand View Research, Inc.](#), Bloomberg

In the short term, America must accelerate aggressive stockpiling efforts to ensure sufficient supply of rare earths and other critical minerals in the event of a conflict. Stockpiling can buy time for the United States to increase critical mineral production or shift supply chains in the event the PRC cuts off supplies. In 1975, the United States created the Strategic Petroleum Reserve to hedge against major oil shortages caused by supply shocks in the Middle East.⁶⁹ To secure access to today's strategic resources, the DoD should lead an aggressive stockpiling effort to guarantee rare earth and magnet supply to major defense programs by 2025.⁷⁰ Once supply for defense platforms is guaranteed, the United States should stockpile minerals and magnets for green technologies. For non-defense needs, the United States should explore friend-shoring supply chains with trusted partners and create localization plans to create regional economies of scale.⁷¹ A good example of this is the United States partnering with other countries to diversify mineral supply chains, jointly offering countries in Africa, Latin America, and elsewhere a better value proposition for mining and processing contracts than PRC-backed competitors.⁷²

The United States should invest in next-generation battery technologies to offset China's dominance in lithium-ion technology. Lithium-based batteries are expensive⁷³ and cells are difficult to transport due to safety concerns.⁷⁴ Investing in new forms of non-lithium battery technology, such as molten-salt batteries, offers a potential opportunity to leapfrog the PRC's bet on aging lithium-ion technology and reduce dependence on critical minerals produced and processed in China.⁷⁵

(2022). Microelectronics could become a trillion-dollar market by the end of the decade. Semiconductor shortages trimmed one percent off the U.S. GDP in 2021, but a supply shock due to a military contingency could be orders of magnitude worse. Ondrej Burkacky, et al., [The Semiconductor Decade: A Trillion-Dollar Industry Strategies to Lead in the Semiconductor World](#), McKinsey (2022); Jordan Fabian, [Biden Aide Deese Says Semiconductor Shortage Cost 1% of U.S. GDP](#), Bloomberg (2022); Antonio Varas, et al., [Strengthening the Global Semiconductor Value Chain in an Uncertain Era](#), Boston Consulting Group & Semiconductor Industry Association at 39-47 (2021).

69 [Strategic Petroleum Reserve](#), U.S. Department of Energy (last accessed 2022).

70 Emily de La Bruyère & Nathan Picarsic, [Elemental Strategy: Countering the Chinese Communist Party's Efforts to Dominate the Rare Earth Industry](#), Foundation for the Defense of Democracies (2022).

71 Megan Lamberth, et al., [The Tangled Web We Wove: Rebalancing America's Supply Chains](#), Center for a New American Security at 11 (2022).

72 [Minerals Security Partnership Media Note](#), U.S. Department of State (2022).

73 Michael Greenfield, [Is LFP Still the Cheaper Battery Chemistry After Record Lithium Price Surge?](#), S&P Global (2022).

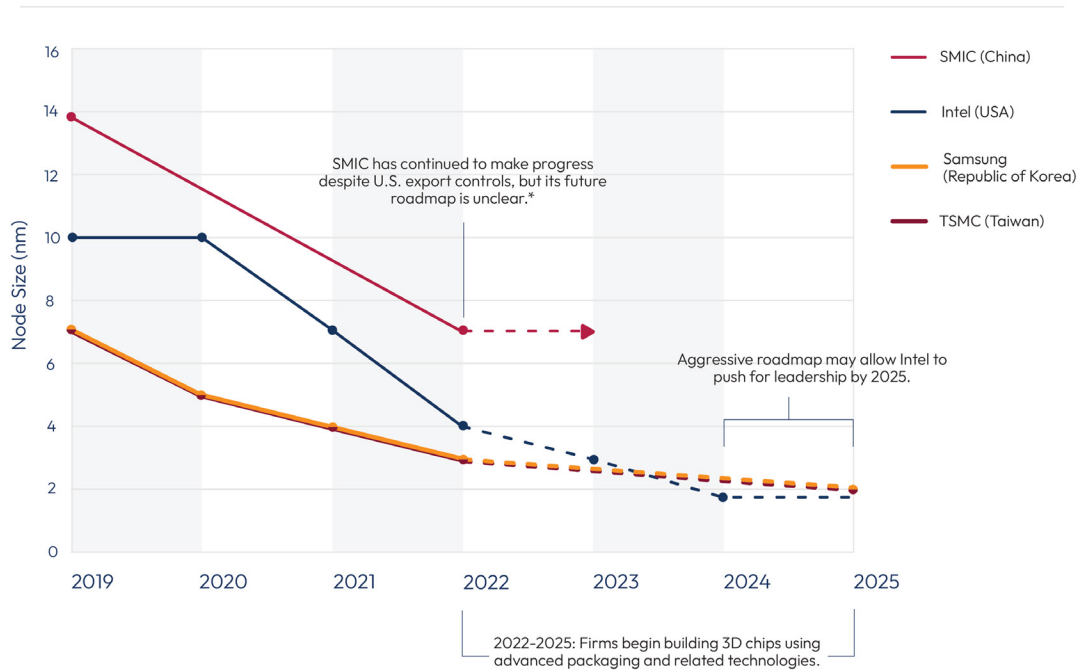
74 Yuqing Chen, et al., [A Review of Lithium-Ion Battery Safety Concerns: The Issues, Strategies, and Testing Standards](#), Journal of Energy Chemistry (2021).

75 Energy Report Part 1: Energy Storage, TechNext (2022) (*SCSP-commissioned work product*).

Regaining American Leadership in Microelectronics

The United States does not currently produce any leading-edge chips, but two trends have created a critical mid-decade window to address this gap.⁷⁶ First, semiconductor giants Intel, Samsung, and Taiwan Semiconductor Manufacturing Company (TSMC) each have begun constructing leading-edge fabs in the United States, though their scale and success depends in part upon the incentives provided by the CHIPS and Science Act.⁷⁷ An accelerated implementation plan would increase the odds of success. Given higher building and operating costs, long-term incentives – especially tax provisions – are necessary to ensure America remains competitive in semiconductors through 2030.⁷⁸ Second, Intel’s aggressive roadmap may potentially allow it to compete at the leading-edge with Taiwan-based TSMC and South Korea-based Samsung by 2025.⁷⁹

State-of-the-Art Semiconductor Manufacturing by Firm: 2019-2025



*SMIC’s 7nm node has entered low-volume production, but the company remains at least two generations behind its competitors. Node sizes for 2022-2025 are projections and reflect firm roadmaps. Node size reflects estimated first year of mass production.

76 Ina Fried, [Interview: Commerce Secretary on U.S. Chip Crisis](#), Axios (2021).

77 Pub. L. 117-167, [The CHIPS and Science Act of 2022](#) (2022).

78 Antonio Varas, et al., [Government Incentives and US Competitiveness in Semiconductor Manufacturing](#), Boston Consulting Group & Semiconductor Industry Association at 14-20 (2020).

79 Dylan Martin, [TSMC’s 2025 Timeline for 2nm Chips Suggests Intel Gaining Steam](#), The Register (2022).

The United States runs the risk of building semiconductor fabs but not having enough engineers to run them. Federal funding can help address this gap. America must invest in its microelectronics workforce.⁸⁰ The country could face a talent gap upwards of 70,000 chip workers in the coming years,⁸¹ and chipmakers have identified this gap as a core obstacle to expanding their U.S. operations.⁸² Federal incentives can help the nation address this shortage.⁸³ The CHIPS and Science Act includes \$200 million to jump-start workforce training, but meeting demand will require sustained funding beyond this initial infusion, as well as additional H1-B visas for foreign engineers.⁸⁴

The United States must ensure that post-Moore's Law chips are designed and built in America. Policymakers should provide incentives to chip startups working to invent the future. As the chip industry nears the end of Moore's Law, the breakthrough that pushes computing to a new paradigm may well come from a startup, rather than an established player. But compared to other industrialized nations, the United States is an unfriendly place for new chip firms.⁸⁵ Policymakers should leverage the CHIPS and Science Act to lower costs and barriers to entry for semiconductor startups. The United States should focus on programs that make it cheaper and faster to transition from prototyping to high volume manufacturing.

American companies, and those in allied nations, have enabled the PRC's chip breakthroughs. The United States and its allies must take stronger actions to block Beijing's access to advanced chips. China is powering its AI ambitions and military modernization with advanced chips designed and built by firms based in the United States and allied countries.⁸⁶ Policymakers must keep export controls and other policies current to the technology and threat, then place the onus on firms to demonstrate that sales of cutting-edge chips to the PRC do not boost Beijing's military modernization and human rights abuses. Meanwhile, the United States has worked with the Netherlands to cut off supply

80 Will Hunt, [Reshoring Chipmaking Capacity Requires High-Skilled Foreign Talent: Estimating the Labor Demand Generated by CHIPS Act Incentives](#), Center for Security and Emerging Technology (2022).

81 Stephanie Yang, [Chip Makers Contend for Talent as Industry Faces Labor Shortage](#), The Wall Street Journal (2022); [How the U.S. Can Reshore the Semiconductor Industry](#), Eightfold.AI (2022).

82 Margaret Harding McGill, [Chip Makers Feel Labor Market Squeeze](#), Axios (2022).

83 [Winning the Future: A Blueprint for Sustained U.S. Leadership in Semiconductor Technology](#), Semiconductor Industry Association at 13-14 (2019).

84 Will Hunt, [Reshoring Chipmaking Capacity Requires High-Skilled Foreign Talent: Estimating the Labor Demand Generated by CHIPS Act Incentives](#), Center for Security and Emerging Technology at 11-12 (2022).

85 Dylan Patel, [Why America Will Lose Semiconductors – Tangible Bi-Partisan Solutions for Solving a National Security Crisis](#), SemiAnalysis (2022).

86 Ryan Fedasiuk, et al., [Silicon Twist: Managing the Chinese Military's Access to AI Chips](#), Center for Security and Emerging Technology (2022).

of specialized extreme ultraviolet lithography (EUV) machines to PRC firms,⁸⁷ but these measures are not enough to slow down Beijing's drive for self-sufficiency.⁸⁸ In coordination with allies, the United States must block China's access to semiconductor manufacturing equipment and restrict the transfer of expertise, know-how, and capital that helps PRC chip startups reach scale.⁸⁹

Preserve: U.S. Financial Leadership in the Digital Age

America's global leadership in finance is a key pillar of its national power, underpinning the prosperity of U.S. businesses and everyday Americans, as well as Washington's ability to impose sanctions and shape global markets. The race to invent the future of money through digital currencies and payments platforms is also a race to preserve this vital advantage, set international payment and data standards, and determine whether democratic values govern the global financial system. The U.S. dollar maintains significant institutional and structural advantages that the renminbi is unlikely to displace in the medium term.⁹⁰ However, U.S. fiscal, monetary, and regulatory missteps, combined with a concerted push by the PRC, could undermine confidence in U.S. financial leadership and lead to a fragmented global financial system.

The United States must lead in financial technology innovation to maintain the primacy of the U.S. dollar. The emergence of new financial technologies (fintech) – such as Central Bank Digital Currencies (CBDCs), cryptocurrencies, and payment systems – raises questions as to the long-term dominance of the U.S. dollar. Fintech could have considerable implications for illicit finance, regulatory regimes, traditional intermediaries (such as banks and brokers), and systemic financial risk. To strike the right balance between innovation and risk mitigation, the United States should create regulations governing cryptocurrency-related digital security, liability, and business and disclosure practices that provide clarity to investors and innovators and ensure financial stability, transparency, and consumer protections. A clear, innovation-friendly regulatory regime can also guide international standards for use and regulation of cryptocurrencies.

The United States should improve the efficiency of dollar-based payments infrastructure to counter the PRC's renminbi-based electronic payments platforms. The PRC has set

87 Stu Woo & Yang Jie, [The PRC Wants a Chip Machine From the Dutch. The U.S. Said No](#), The Wall Street Journal (2021).

88 Jenny Leonard, et al., [China's Chipmaking Power Grows Despite US Effort to Counter It](#), Bloomberg (2022).

89 Andre Barbe & Will Hunt, [Preserving the Chokepoints: Reducing the Risks of Offshoring Among U.S. Semiconductor Manufacturing Equipment Firms](#), Center for Security and Emerging Technology (2022); Stephen Nellis, [The U.S. Weighs a Broader Crackdown on Chinese Chipmakers](#), The Information (2022).

90 Eswar Prasad, [China's Digital Currency Will Rise But Not Rule](#), Brookings (2020).

its sights on undermining the dollar's dominant role in global finance.⁹¹ Without a flexible exchange rate, an open capital account, and widely trusted public institutions, the PRC will struggle to establish the renminbi as a global reserve currency rivaling the dollar, or even its nearest peers including the euro, yen, and pound sterling.⁹² At the same time, Beijing's efforts could erode the dollar's position in settling international transactions and hand the PRC a first-mover advantage in setting standards for digital finance and related data platforms. The PRC is deploying currency innovations, like the electronic renminbi (e-CNY), and renminbi-based alternative payment channels, such as the Cross-Border Interbank Payment System (CIPS)⁹³ to increase transaction efficiency, reduce vulnerability to U.S. sanctions, and harvest data at home and abroad.⁹⁴ The United States can support innovations that reduce transaction costs and improve efficiency and resilience in dollar-based and U.S.-led payment systems, such as those run by the Federal Reserve,⁹⁵ the Society for Worldwide Interbank Financial Telecommunication (SWIFT), and the Clearing House Interbank Payment System (CHIPS).⁹⁶

The U.S. should seek to set international standards and regulations for Central Bank Digital Currencies and dollar-pegged stablecoins that align with democratic values and preserve financial stability. CBDCs – digital forms of money issued and backed by a central bank⁹⁷ – and stablecoins – privately issued digital currencies with an exchange value pegged to a fiat currency – carry potential benefits and risks. While they could improve inclusion and efficiency within the financial system and even deepen the dollar's global role, they might also create new cybersecurity, privacy, and financial stability vulnerabilities. As the PRC pilots its own autocratic CBDC⁹⁸ initiative, the United States has a unique opportunity to set international standards for CBDCs and stablecoins compatible with democratic values, allowing private sector innovators to compete to develop the best technical solution for a

91 Rush Doshi, [The Long Game: China's Grand Strategy to Displace American Order](#), Oxford University Press at 247-250 (2021); PRC officials are quoted as criticizing the "monopolistic position" of the U.S. dollar. See Jonathan Kirschner, [The Great Wall of Money](#), Cornell University Press at 223 (2014).

92 Eswar Prasad, [China's Digital Currency Will Rise But Not Rule](#), Brookings (2020); Eswar Prasad, [The Dollar Trap](#), Princeton University Press at 231-240 (2014).

93 Eswar Prasad, [The Future of Money](#), Harvard University Press at 252-309 (2021).

94 Testimony of Samantha Hoffman before the U.S.-China Economic and Security Review Commission, [An Assessment of the CCP's Economic Ambitions, Plans, and Metrics of Success, Panel Four on "China's Pursuit for Leadership in Digital Currency"](#) (2021).

95 [About the FedNow Service](#), The Federal Reserve (last accessed 2022).

96 These payment systems include the Federal Reserve, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), and the Clearing House Interbank Payment System (CHIPS). See Russell Wong, [What is SWIFT, and Could Sanctions Impact the U.S. Dollar's Dominance?](#), Federal Reserve Bank of Richmond (2022).

97 [What is a Central Bank Digital Currency?](#), Board of Governors of the Federal Reserve System (2021).

98 Testimony of Samantha Hoffman before the U.S.-China Economic and Security Review Commission, [An Assessment of the CCP's Economic Ambitions, Plans, and Metrics of Success, Panel Four on "China's Pursuit for Leadership in Digital Currency"](#) (2021).

CBDC within those parameters.

The United States could establish a National Security Commission on Digital Finance (NSCDF) to study the impact of digital finance on national security and economic competitiveness. The subject of digital finance combines many individually complex topics: banking, technology, monetary policy, geopolitics, data privacy, and data sovereignty issues. Building on the ongoing policy processes mandated by the Executive Order on Ensuring Responsible Development of Digital Assets,⁹⁹ an NSCDF could convene private stakeholders and public officials to present findings and make recommendations to the President and Congress on digital finance.

Intellectual Property Rights: A Cornerstone of the Innovation Economy

As emerging technologies produce new forms of value, the United States should update its intellectual property (IP) regime to keep up. Robust IP rights underpin the U.S. economy's vibrant innovation ecosystem and incentivize value creation. Yet the United States has not modernized IP laws and policies to keep pace with rapid innovations in AI, fintech, biotechnology, and other sectors. To address this gap while safeguarding U.S. national security and promoting economic competitiveness,¹⁰⁰ four areas should be prioritized:

- **Determine** whether AI that generates inventions and creations should be entitled to IP protection.
- **Clarify** the current patent eligibility doctrine that has created enormous uncertainty surrounding patent protections for cutting-edge computer-implemented and biotechnology inventions. A lack of clarity deters investments in high-risk innovation.¹⁰¹

⁹⁹ EO 14067, [Ensuring Responsible Development of Digital Assets](#) (2022).

¹⁰⁰ [Final Report](#), National Security Commission on Artificial Intelligence at 201-207 (2021); Kevin Madigan & Adam Mossoff, [Turning Gold to Lead: How Patent Eligibility Doctrine Is Undermining U.S. Leadership in Innovation](#), *George Mason Law Review* (2019).

¹⁰¹ Testimony of Judge Paul R. Mochel Before the Subcommittee on Intellectual Property, U.S. Senate Committee on the Judiciary, [The State of Patent Eligibility in America: Part I](#) (2019).

- **Examine** the need for IP and IP-like protections to incentive creation and sharing of data sets.¹⁰²
- **Collaborate** with allies and partners to promote pro-innovation IP concepts, develop global disincentives for IP theft, and leverage international forums to increase representation for the United States and its allies and partners.¹⁰³

Pushback: Coercive Economic Statecraft

Rebuilding America’s economic engine is essential to winning the competition, but without pushing back against Beijing’s economic malpractice, the United States will continue to fall behind. Each year, China inflicts economic damage on the United States that far exceeds the annual economic output of Virginia, or the annual sales of the entire global semiconductor market.¹⁰⁴ The PRC has harnessed U.S. and allied technology, capital, and know-how to power its techno-economic ambitions and military modernization.¹⁰⁵ America must join hands with its allies and partners, leveraging the tools of economic statecraft to fill gaps and push back aggressively against the threats the PRC poses to American economic and national security.

102 [Public Views on Artificial Intelligence and Intellectual Property Policy](#), U.S. Patent and Trademark Office (2020).

103 In 2020, the United States successfully rallied allies and partners to support a Singaporean candidate, Daren Tang, as Director General for the World Intellectual Property Organization, trumping efforts by the PRC – the world’s leading infringer of IP rights – to install its own candidate. See Daniel F. Runde, [Trump Administration Wins Big with WIPO Election](#), The Hill (2020).

104 The annual cost of IP theft, one vector of China’s economic malpractice, has been estimated between \$225 to \$600 billion. See [Findings Of The Investigation Into China’s Acts, Policies, And Practices Related To Technology Transfer, Intellectual Property, And Innovation Under Section 301 Of The Trade Act Of 1974](#), Office of the U.S. Trade Representative (2018). Counting other vectors – including subsidies, market distortions, market access restrictions, technology transfer, etc. – the number is significantly higher, but a single estimate does not exist. For comparison, Virginia’s annual economic output was approximately \$492 billion in 2021. See [Real Gross Domestic Product \(GDP\) of the federal state of Virginia from 2000 to 2021](#), Statista (2022). Global semiconductor sales in 2020 totaled \$440.4 billion. See [Global Semiconductor Sales Increase 24% Year-to-Year in October; Annual Sales Projected to Increase 26% in 2021, Exceed \\$600 Billion in 2022](#), Semiconductor Industry Association (2021).

105 [Military-Civil Fusion and the People’s Republic of China](#), U.S. Department of State (2020).

The Myth of a Level Playing Field: Examples of PRC Economic Malpractice

The PRC pursues distortionary economic policies on a scale that harms U.S. companies and workers and renders fair competition in international markets impossible. Examples include IP theft, forced technology transfer, cyber-enabled commercial espionage, market access restrictions, and industrial subsidies that far exceed what other governments provide and contravene China's WTO commitments.¹⁰⁶

- The PRC is the world's leading perpetrator of IP theft, costing the United States up to \$600 billion annually.¹⁰⁷ For comparison, this exceeds Virginia's total economic output (\$591 billion in 2021).¹⁰⁸
- The PRC is the largest origin economy for counterfeit and pirated goods, accounting for 92 percent of U.S. seizures in fiscal year 2019.¹⁰⁹
- Between 1998 and 2018, Huawei received \$75 billion in government financial support – subsidies designed to undercut rivals and drive out competition. China's subsidy and export credit practices violate its WTO commitments. For comparison, Cisco has received \$44.5 million in U.S. Government assistance since 2000.¹¹⁰
- The growing trade deficit with China cost the United States an estimated 3.7 million jobs between 2001 and 2018. The computer and electronic parts industry was hit the hardest, and three Congressional districts in Silicon Valley lost roughly 12 to 20 percent of total jobs in the districts.¹¹¹

106 [2021 Special 301 Report](#), Office of the U.S. Trade Representative (2021). On industrial subsidies, see Gerard DiPippo et al., [Red Ink: Estimating Chinese Industrial Policy Spending in Comparative Perspective](#), Center for Strategic and International Studies (2022).

107 [Findings Of The Investigation Into China's Acts, Policies, And Practices Related To Technology Transfer, Intellectual Property, And Innovation Under Section 301 Of The Trade Act Of 1974](#), Office of the U.S. Trade Representative at Appendix C at 9 (2018).

108 [Gross Domestic Product: All Industry Total in Virginia](#), Federal Reserve Bank of St. Louis (2022).

109 [2021 Special 301 Report](#), Office of the U.S. Trade Representative at 16 (2021).

110 Chuin-Wei Yap, [State Support Helped Fuel Huawei's Global Rise](#), Wall Street Journal (2019). See also Stephen Ezell, [False Promises II: The Continuing Gap Between China's WTO Commitments and Its Practices](#), Information Technology and Innovation Foundation (2021).

111 Robert E. Scott & Zane Mokhiber, [Growing China Trade Deficit Cost 3.7 million American Jobs Between 2001 and 2018](#), Economic Policy Institute at 19-20 (2020).

The PRC's growing track record of economic malpractice means that a new approach is required. Attempts to convince the PRC to reign in its behaviors and compete on a “level playing field” have fallen flat.¹¹² The last two decades have seen a more aggressive Beijing willing to break its international commitments, bend its corporate champions to the requirements of the state and military, and bully its trading partners.¹¹³ If left unchecked, the PRC's pattern of behavior will inflict even more damage on higher value-added sectors and threaten national security in the United States and other advanced economies. To push back, America, in coordination with its allies and partners, must sharpen the tools of coercive economic statecraft and change incentives for Western companies and investors.

The United States and its allies must pursue collective economic self-defense. Beijing has made its choice clear¹¹⁴ – it seeks a one-way decoupling strategy to increase the world's dependence on China while reducing China's dependence on the world for critical technologies.¹¹⁵ For the United States and its allies, collective economic self-defense offers a more realistic and sustainable policy approach than ever-deepening entanglement and vulnerability to Beijing. This approach will put a price tag on the negative externalities that result from the PRC's unfair and predatory behaviors, passing the costs on to the offender.

The United States should work together with allies and partners wherever possible to maximize leverage and eliminate gaps that the PRC can exploit.¹¹⁶ The United States will often have to lead the way, setting an example for allies and partners to follow. America's large, diversified economy and low trade dependence on China (with goods exports to China equivalent to only 0.5 percent of U.S. GDP)¹¹⁷ means it can weather potential disruptions.

112 For example, in multilateral negotiations at the WTO since China's accession in 2001, and the annual U.S.-China Strategic and Economic Dialogue, the PRC repeatedly committed to make market-oriented reforms but largely failed to do so. See [2021 Report to Congress on China's WTO Compliance](#), Office of the U.S. Trade Representative at 7 (2022).

113 For more information on PRC economic coercion, see [China's Global Sharp Power Project](#), Hoover Institution; Peter Harrell, et al., [China's Use of Coercive Economic Measures](#), Center for a New American Security (2018); Adam Segal, [Huawei, 5G, and Weaponized Interdependence in the Uses and Abuses of Weaponized Interdependence](#), Brookings Institution Press (2021); Thomas Cavanna, [Coercion Unbound? China's Belt and Road Initiative in the Uses and Abuses of Weaponized Interdependence](#), Brookings Institution Press (2021).

114 For assessments of CCP intentions based on authoritative, primary source documents, see Rush Doshi, [The Long Game: China's Grand Strategy to Displace American Order](#) (2021); Peter Mattis, [The Party Congress Test: A Minimum Standard for Analyzing Beijing's Intentions](#), War on the Rocks (2019); Daniel Tobin, [How Xi Jinping's New Era Should Have Ended U.S. Debate on Beijing's Ambitions](#), Center for Strategic and International Studies (2020).

115 On PRC policies to reduce reliance on advanced democracies while increasing their reliance on the PRC – recently dubbed “[dual circulation](#)” – see, for example, [Testimony of Matt Pottinger Before the United States-China Economic and Security Review Commission](#) (2021); Rush Doshi, [The Long Game: China's Grand Strategy to Displace American Order](#), at 134-156 (2021). For an authoritative CCP policy document, see [Translation: Outline of the People's Republic of China 14th Five Year Plan](#), Center for Security and Emerging Technology (2021).

116 Aaron Friedberg, [Getting China Wrong](#), Polity Press at 171-172 (2022).

117 U.S. GDP in 2020 was just over \$20 trillion. [GDP \(Current US\\$\) - United States](#), World Bank (2021). U.S. goods exports to China in 2020 were \$123 billion – equivalent to half a percent of U.S. GDP. [2021 State Export Report](#), The U.S.-China Business Council (2021). The United States is the [world's largest exporter of services](#), but PRC market access restrictions means many U.S. services are blocked and thus

In many industries the United States remains the largest market,¹¹⁸ and in many others it is by far the most lucrative and accessible one.¹¹⁹ The United States should be prepared to leverage access to its enormous and profitable market to redirect critical supply chains to domestic and ally- and partner-based production.

The objectives of this approach should be twofold:

- **Diversification**

The United States should form plurilateral frameworks with allies and partners to diversify supply chains, maximizing collective leverage vis-a-vis the PRC.¹²⁰ Critics will frame such efforts as “decoupling” — an overwrought term that implies a sudden and total severing of economic ties. Rather, diversifying should proceed in a progressive and targeted fashion, starting with decisive steps to disentangle from the PRC where interdependence poses the greatest risks — especially dual-use technologies and critical infrastructure.

- **Denial**

As U.S. cash, technologies, and expertise flow into the PRC, American consumers, investors, and innovators end up reinforcing PRC malpractice at the expense of the home front, either knowingly or not. The United States and its allies should also seek to deny these flows to the PRC when they would contribute to China’s military development, fundamentally undermine the competitiveness of rule-of-law economies in high-tech sectors (such as semiconductors, aerospace, and biotechnology), or contribute to the PRC’s human rights abuses, including genocide and crimes against humanity in Xinjiang.¹²¹ As an example, U.S. venture capital firms, chip industry giants, and other investors participated in 58 investment deals with China’s semiconductor industry from 2017 to present, raising billions of dollars for PRC chip startups and helping them reach scale¹²² — accelerating China’s progress in a sector where it is important for America to remain ahead. In another example, U.S. and European companies and research institutions have helped

exports are much lower than they would be if China were a normal economy.

118 [Telecom Equipment Market Size is Projected to Grow at an 11.23% CAGR by 2025](#), Market Research Future (MRFR) (2021).

119 Rick Switzer, U.S. National Security Implications of Microelectronics Supply Chain Concentrations in Taiwan, South Korea and The People’s Republic of China, OCEA Occasional White Paper (2019).

120 “Plurilateral” groupings are agreements between two or more countries, but fewer than all members of an existing organization. See [Delivering Plurilateral Trade Agreements within the World Trade Organization](#), UK Trade Policy Observatory at 5 (2021).

121 [2021 Report on International Religious Freedom: China – Xinjiang](#), U.S. Department of State (2022).

122 Kate O’Keefe, et al., [U.S. Companies Aid China’s Bid for Chip Dominance Despite Security Concerns](#), Wall Street Journal (2022).

Beijing build genomic surveillance programs for use in discriminatory law enforcement and political control against population in China and around the world.¹²³ These activities should be banned.

The United States must update export controls for the age of emerging technology, strengthen existing inbound investment screening processes, and establish an effective outbound investment screening framework. Today, critical technologies built in U.S. laboratories – and billions of dollars of U.S. capital – flow into the PRC, accelerating China’s military modernization and technological progress in sectors where America must remain ahead.¹²⁴ Stronger export control and investment screening measures are needed to ensure that the United States is not investing in its own decline.

Stronger export control and investment screening measures are needed to ensure that the United States is not investing in its own decline.

- **Export Controls**

Despite recent reforms, U.S. export controls are failing to stem the flow of advanced technology to the PRC.¹²⁵ The Department of Commerce must identify and implement new controls on emerging technologies, pursuant to its obligations under Export Control Reform Act of 2018.¹²⁶ Commerce should close the gaps in its current licensing policy to better enforce the controls introduced against PRC state champions, such as Huawei.¹²⁷ Internationally, the United States should lead in the creation of a new multilateral export controls regime that addresses the contemporary challenges of national security, economic security, MCF,¹²⁸ and human rights issues, including the PRC genocide in Xinjiang.¹²⁹ A PRC-focused approach can build off of the momentum and precedent created by the U.S. and

123 Sui-Lee Wee & Paul Mozur, [China Uses DNA to Map Faces, with Help from the West](#), New York Times (2019); Emile Dirks & James Liebold, [Genomic Surveillance](#), Australian Strategic Policy Institute (2020).

124 Kate O’Keefe, et al., [U.S. Companies Aid China’s Bid for Chip Dominance Despite Security Concerns](#), Wall Street Journal (2022).

125 [U.S. Export Controls and China](#), Congressional Research Service (2022).

126 Testimony of Nazak Nikakhtar before the Senate Select Committee on Intelligence, [Threats to U.S. National Security: Countering the PRC’s Economic and Technological Plan for Dominance](#) (2022).

127 James Mulvenon, [Seagate Technology and the Case of Missing Huawei FDPR Enforcement](#), Lawfare (2022).

128 [Military–Civil Fusion and the People’s Republic of China](#), U.S. Department of State (2020).

129 Kevin Wolf & Emily S. Weinstein, [COCOM’s Daughter?](#), WorldECR (2022).

allied coordination on the sweeping export controls on critical technological inputs in Russia's industrial base.¹³⁰

- **Investment Screening**

America must craft common-sense guardrails to curb the flow of know-how and investment dollars to China's military and techno-economic engine and to incentivize investment flows into the United States and its allies instead. The Federal Government could take action by expanding the jurisdiction of CFIUS to review inbound investments in a wider set of technologies where adversary access would threaten U.S. national security¹³¹ and include oversight of more joint ventures and minority positions in investments.¹³² The United States must also establish an outbound investment screening process that can screen and block the flow of capital and know-how into its adversaries' high-tech sectors (such as semiconductors, aerospace, and biotechnology) that undermine U.S. economic competitiveness and national security.

The United States and its allies should apply a "rebuttable presumption" – a standard innovatively applied policy innovation from the Uyghur Forced Labor Prevention Act (UFLPA) – to reduce exposure to the PRC in areas where U.S. private sector entanglement risks harming national security or advancing PRC strategic technology capabilities. For nearly a century, U.S. law has prohibited the import of products made with forced labor.¹³³ The PRC's lack of transparency complicates U.S. customs authorities' ability to determine which imports from China meet that criterion. The logic of the UFLPA, which entered into force this year, is that the PRC's extensive forced labor programs, restricted access to the Xinjiang Uyghur Autonomous Region (XUAR), and denial of routine supply chain reviews¹³⁴ require the U.S. Government to shift the burden of proof to companies with XUAR-connected supply chains to show that they were not using forced labor in order to import products into the United States.¹³⁵ This principle, known as "rebuttable presumption," should be applied to other high-risk areas beyond forced labor. For example, a rebuttable presumption could address partnerships with entities linked to MCF and talent

¹³⁰ Emily S. Weinstein, [Making War More Difficult to Wage](#), Foreign Affairs (2022).

¹³¹ Emma Rafaelof, [Unfinished Business: Export Control and Foreign Investment Reforms](#), U.S.-China Economic and Security Review Commission (2021).

¹³² David Hanke, [Hearing on U.S.-China Relations in 2021: Assessing Export Controls and Foreign Investment Review](#), U.S.-China Economic and Security Review Commission (2021).

¹³³ Cathleen D. Cimino-Isaacs, [Section 307 and Imports Produced by Force Labor](#), Congressional Research Service (2022).

¹³⁴ Haley Byrd Wilt, [How the Uyghur Forced Labor Prevention Act Became Law, Part 1](#), The Dispatch (2022).

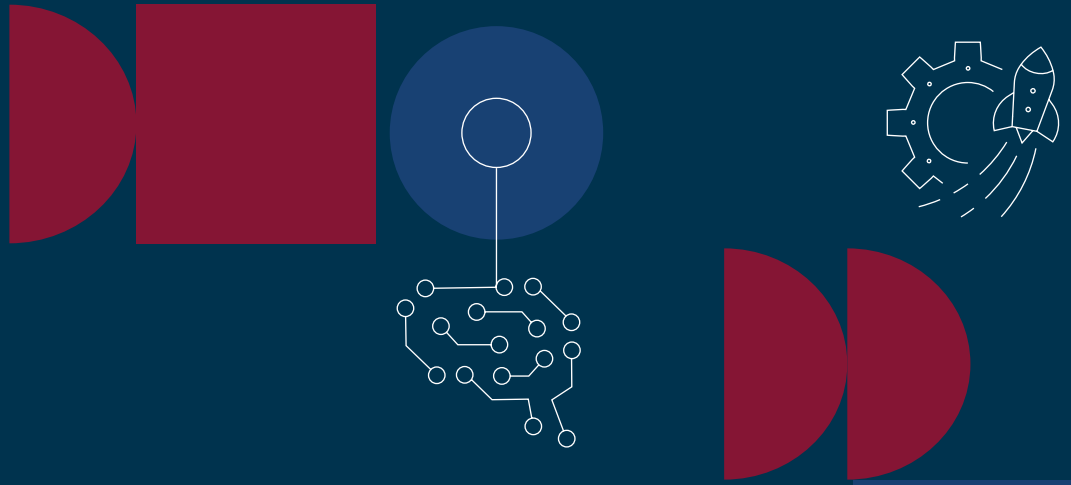
¹³⁵ See [Uyghur Force Labor Protection Act](#), U.S. Customs and Border Protection (2022).

and technology transfer programs. This would not ban the interactions outright, but would place the burden of proof on the U.S. person wishing to conduct an activity to show that it is not harmful to national security. The rebuttable presumption would be much more powerful if applied alongside allies and partners.

An American Approach to AI Governance

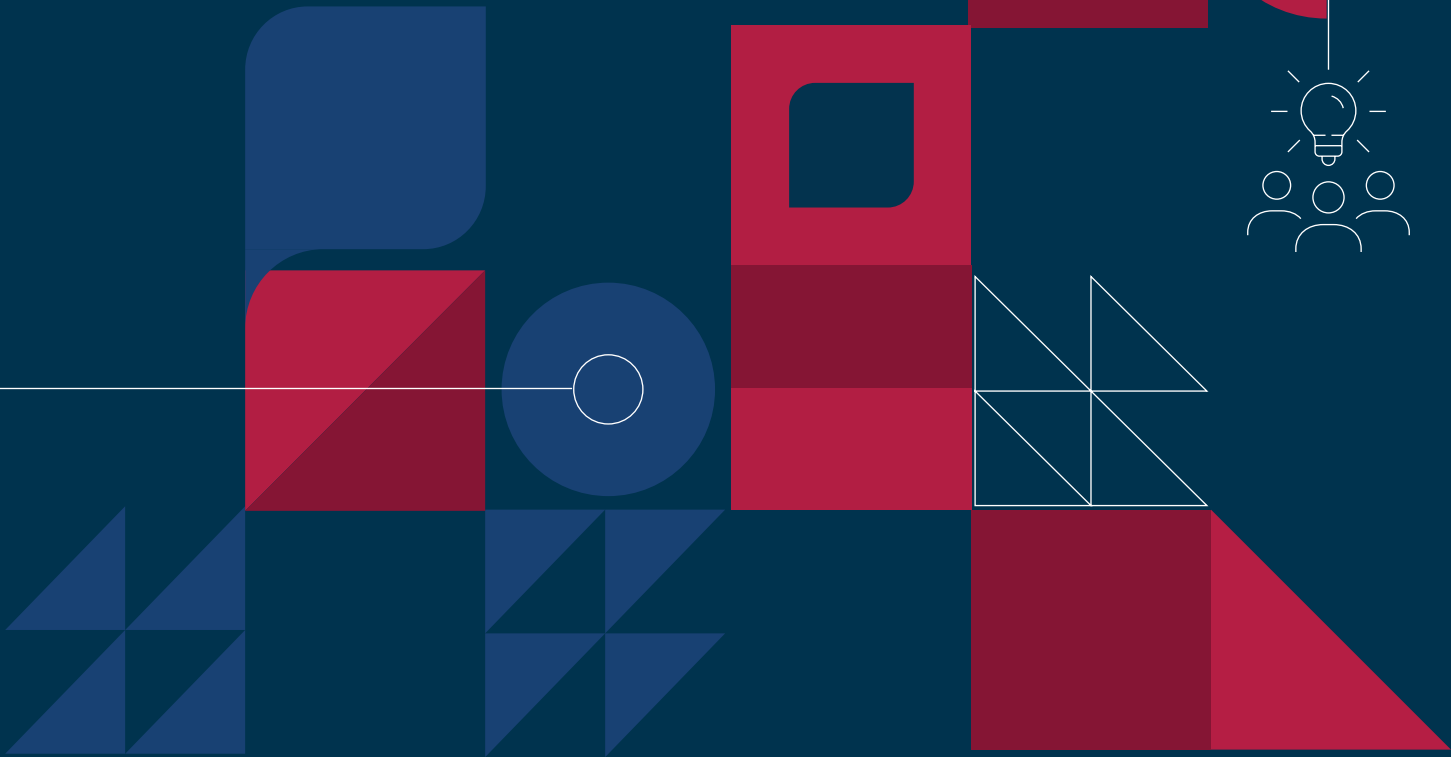
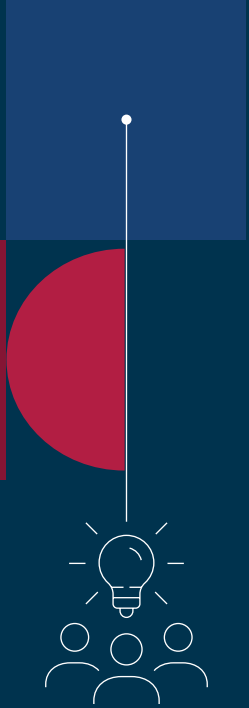
Mid-Decade Challenges to National Competitiveness

03



• **Four Principles for American AI Governance**

• **Six Decisive Enablers for Increasing Justified Public Confidence in AI**



CHAPTER 3

An American Approach to AI Governance

Technology governance is the underappreciated factor in technology competition. The societies that harness new technologies to improve their standards of living, grow their economies, and strengthen their security will be best positioned to win a long-term contest. New technologies can also be deeply destabilizing, harm individuals and communities, undermine confidence in government, and engender a backlash that stifles innovation. The governments that encourage technology innovation while ensuring it is accomplished safely, responsibly, and with public support will be at a competitive advantage and offer a model for the rest of the world. Success in striking the balance between driving innovation and minimizing harm hinges on the norms, rules, frameworks, regulations, and laws that determine how technologies are applied.

Artificial intelligence is the technology posing the most immediate, vexing, and wide ranging set of governance challenges across the world today. In that respect, getting AI governance right is the key to getting tech governance right. The United States must develop a compelling and workable AI governance model or risk living in a world in which technologies that deeply affect our everyday lives do not reflect our values and where we cede innovation leadership to others. By 2025, in the absence of American leadership, much of the world might very well be living either under digital norms dictated by the authoritarian CCP or under overly-restrictive regulatory regimes set up in response to AI skepticism and fear.

In a systems contest to demonstrate the superiority of democracy, using AI to broadly benefit society will be a competitive advantage. The useful applications of AI are wide-ranging and expanding. AI is enhancing decision making across many areas – for cybersecurity, factory and supply chain optimization, medical image processing, and more. AI is enabling physical platforms to become increasingly autonomous, and the trend toward more

sophisticated autonomy is clear. Consider warehouse robotics, precision agriculture, self-driving cars, and ocean transport. Most significantly, AI is accelerating scientific discovery and engineering, for example with protein folding, drug discovery, fusion magnet controls, and breakthroughs in astronomy.

To capitalize on the potential of AI for social benefit, the United States must govern AI systems wisely. Shaping the development and use of AI will require calibrating the full range of governance mechanisms, regulatory and non-regulatory, to strike the right balance. We should not let the pendulum swing too far in the direction of a singular focus on minimizing risk. Such an extreme would dampen innovation by reducing investment in new inventions and adding impediments to new adoption. We also must not let the pendulum swing too far in the direction of “move fast and break things” when real harm is a possibility. This extreme increases the risks of harm and could produce a backlash leading to a singular focus on risk minimization with heavy-handed regulation. The right balance requires informed risk tradeoff decisions so that we maximize the benefits while minimizing the harms based on the specific uses of AI.

In authoritarian states, these tradeoff decisions are made by the state with no need to gain the consent of the governed. Liberal democracies require respect for human rights and the rule of law. The United States can find a competitive advantage if it illustrates a model of AI governance that upholds democratic values and norms while also supporting innovation, economic growth, and national security interests. The challenge is how to create a broadly shared understanding of the way forward on technology governance that is rights-protecting and innovation-enhancing.

Given the breadth of its impact, competing approaches to technology governance are playing out most sharply in AI. Governments across the ideological spectrum are grappling with how to influence AI advances to serve their societies.¹ The PRC is developing an authoritarian approach.² Some of its regulations may look good on “paper,” and indeed mirror regulations that could be adopted by democracies. But Beijing’s methods of social control reveal its true priorities. In contrast, the EU is attempting to create a democratic model that leverages its regulatory strength to create an ecosystem of trust, alongside

1 For a broad comparison see Johanna Weaver and Sarah O’Connor, [Tending the Tech-Ecosystem: Who should be the tech-regulator\(s\)?](#), Australian National University at 6-7 (2022).

2 China has issued a series of policy documents and policy pronouncements on its governance regime for AI that aligns with its state interests. See Matt Sheehan, [China’s New AI Governance Initiatives Shouldn’t Be Ignored](#), Carnegie Endowment for International Peace (2022); Katharin Tai, et al., [Translation: Guiding Opinions on Strengthening Overall Governance of Internet Information Service Algorithms](#), DigiChina (2021). They tend to focus on regulating the provider organization or outcome with the resulting benefit that they are applicable regardless of technology and resilient to tech changes. See Helen Toner, et al., [Translation: Internet Information Service Algorithmic Recommendation Management Provisions \(Draft for Comment\) Aug. 2021](#), DigiChina (2021).

investments to create an “ecosystem of excellence.”³ But in our assessment, the EU’s regulatory gamble might stifle innovation due to compliance costs and associated burdens for SMEs.⁴ The UK’s AI governance approach is a deliberate attempt to strike a balance – maximizing growth and competition, driving innovation, and protecting its citizens’ rights; it represents an alternative to the EU model but has not yet been implemented through laws and regulations.⁵

The United States cannot promote AI advancements that support its vision of democratic ideals without **comprehensive national strategies** for governing them at home.

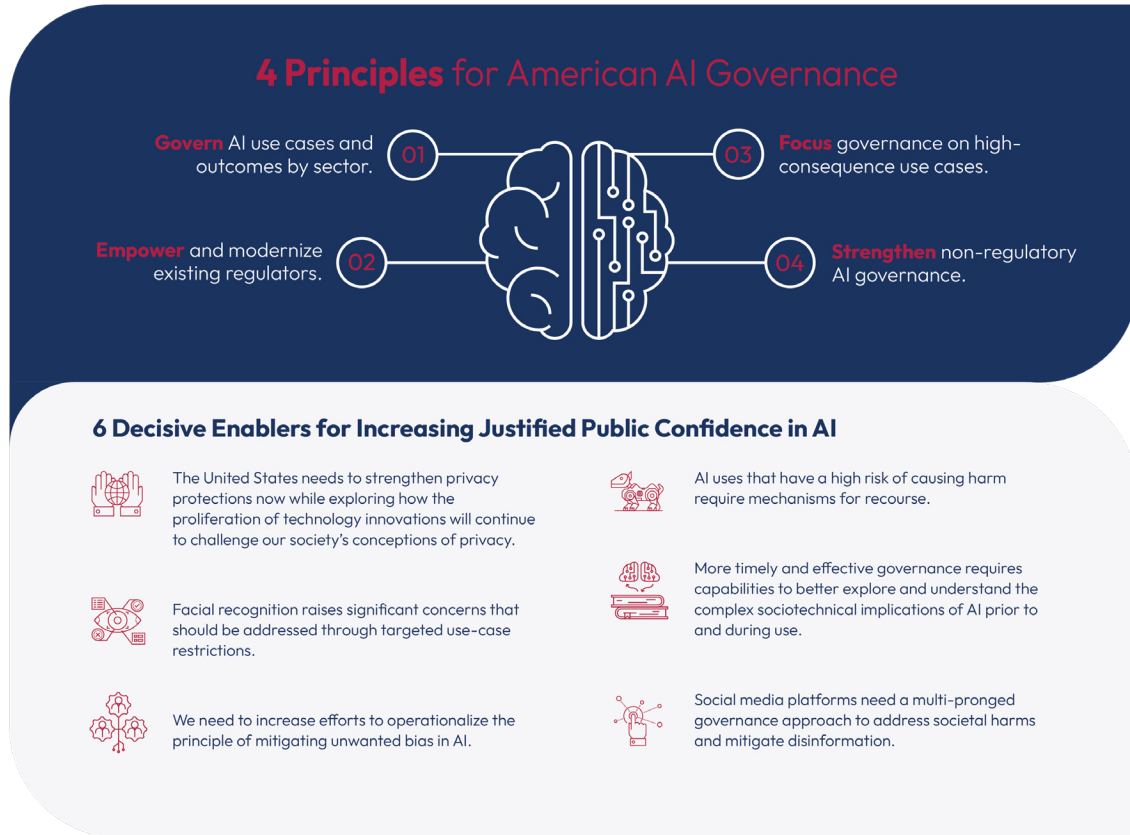
It is time for an American approach that is innovation-friendly and still responsive to legitimate concerns about harms of AI applications. Today, however, the United States does not yet have a coherent strategy to present to the world. The United States cannot promote AI advancements that support its vision of democratic ideals without comprehensive national strategies for governing them at home. These strategies need to garner public confidence in technology and governing institutions, promote innovation, and lay the foundation for maximizing the opportunities presented by AI-enabled systems.

³ [On Artificial Intelligence - A European Approach to Excellence and Trust](#), European Commission at 3 (2020). The European Union has issued the GDPR and its AI Act is getting closer to being set into law, both of which tilt toward protectionism and arguably do not prioritize innovation. Despite their weaknesses, these laws have the advantage of being the first broad regulatory regime rooted in democratic values that are presented globally. In the past, evidence has shown that the EU’s head start on transnational legislation made it a model for the rest of the world, thereby expanding its regulatory impact. See Jonathan Keane, [From California to Brazil, Europe’s privacy law has created a recipe for the world](#), CNBC (2021). In the present case, it is unclear whether the AI Act’s so-called “[Brussels effect](#)” will dictate companies’ new AI standards. However, another factor that could indirectly lead to the same outcome is compliance costs. It might be costlier to have different operating standards, rather than making the AI Act the standard – especially in the absence of competing legislation.

⁴ See Evangelos Razis, [Europe’s Gamble on AI Regulation](#), U.S. Chamber of Commerce (2021) (“According to one study sponsored by the European Commission, businesses would need as much as \$400,000 up front just to set up a ‘quality management system.’ Few startups or small and medium-sized businesses can pay this price of admission into the AI marketplace, let alone the additional costs associated with compliance.”) (citing [Study Supporting the Impact Assessment of the AI Regulation](#), European Commission (2021)). While the EU also intends to focus on strengthening innovation, only time will tell whether SME compliance burden concerns are addressed.

⁵ The UK’s national strategy for AI touches on a broad breadth of challenges: emphasizing the need for talent and R&D provisions and mitigating social harm, while ensuring the uptake of innovation adoption. [National AI Strategy](#), UK Secretary of State for Digital, Culture, Media and Sport (2021).

An American Way for AI Governance



Four Principles for American AI Governance

An American way of AI governance should be guided by four principles:

First, govern AI use cases and outcomes by sector. The risks and opportunities presented by AI are inextricably tied to the context in which it is used. Currently, the United States is pursuing sector-specific efforts to regulate AI by adapting existing regulatory frameworks and agencies to address new issues introduced by the adoption of AI.⁶

Although some advocate for broader cross-sector AI regulation,⁷ trying to assign

⁶ Examples include the Food and Drug Administration's rulemaking for machine learning (ML) as a medical device and good ML manufacturing processes, the Federal Aviation Administration's policy on how AI in safety-critical avionics should be addressed in regulation, and the Federal Trade Commission's application of its current regulatory authorities to new commercial uses of AI. [Artificial Intelligence and Machine Learning in Software as a Medical Device](#), U.S. Food and Drug Administration (2021). [Good Machine Learning Practice for Medical Device Development: Guiding Principles](#), U.S. Food and Drug Administration (2021). Chris Wilkinson, et al., [Verification of Adaptive Systems](#), U.S. Federal Aviation Administration (2016). Elisa Jillson, [Aiming for Truth, Fairness, and Equity in Your Company's Use of AI](#), U.S. Federal Trade Commission (2021).

⁷ Anton Korinek, [Why We Need a New Agency to Regulate Advanced Artificial Intelligence](#), Brookings (2021); S.1896, [Algorithmic Justice and Online Platform Transparency Act](#) (2021) (levying requirements for algorithms regardless of sector or use case); H.R. 6580, [Algorithmic](#)

regulatory oversight across broad use cases to a centralized regulator would introduce a range of problems and inefficiencies.⁸ A sector-specific approach is consistent with past American regulatory successes. However, information about AI applications and lessons learned should still be shared across sectors.⁹ Existing structures and processes to facilitate this cross-sector communication should be encouraged and expanded.¹⁰

Second, empower and modernize existing regulators. The United States should rely on its existing constellation of sector-specific regulators,¹¹ which can be equipped to address new regulatory needs raised by AI. Existing regulatory bodies have the sector expertise that allows for tailoring rules, ensuring AI governance complements existing non-AI governance, and assessing impacts.¹² However, we must identify the resources these agencies currently lack to address

Because existing regulatory bodies were created in a different technology era, the **United States needs to modernize** them for the new AI era.

regulatory challenges posed by AI. Because existing regulatory bodies were created in a different technology era, the United States needs to modernize them for the new AI era.¹³

[Accountability Act of 2022](#) (2022) (requiring impact assessments for decision making systems across sectors, such as healthcare, loan approval, and hiring systems).

8 Mariano-Florentino Cuellar & Aziz Z. Huq, [The Democratic Regulation of Artificial Intelligence](#), Knight First Amendment Institute at Columbia University (2022) (“The idea of a single, centralized regulator with wide-ranging power over a new, general-purpose technology doesn’t seem effective either from a political-economy, a historical, or even a constitutional perspective.”).

9 For example, some of the lessons learned about governing the safety-critical aspects of autonomous vehicles are likely relevant to concerns about governing other safety-critical uses of AI in embedded systems such as medical AI.

10 As an example, the National Artificial Intelligence Initiative Act of 2020 states that the [National AI Initiative Committee shall] “coordinate ongoing artificial intelligence research, development, and demonstration activities among the civilian agencies, the Department of Defense and the Intelligence Community to ensure that each informs the work of the others.” See Pub. L. 116-283, [William M. \(Mac\) Thornberry National Defense Authorization Act for Fiscal Year 2021](#), 134 Stat. 3388 §5101(a)(4) (2021).

11 Adoption of AI under existing regulatory authorities is consistent with OMB Memo M-21-06. See Memorandum from Russell T. Vought, Director of the Office of Management and Budget, [Guidance for Regulation of Artificial Intelligence Applications](#), Executive Office of the President of the United States (2020).

12 Sachin Waikar, [Algorithms, Privacy, and the Future of Tech Regulation in California](#), Stanford Institute for Human-Centered AI (2022) (quoting Jennifer Urban) (“Regulation aims to provide guardrails, allowing a robust market to develop and businesses to flourish while reflecting the needs of consumers. Regulators need to understand the business models and whether their actions would be ‘breaking’ something in the industry.”).

13 For example, “[t]hrough the FDA can trace its origins back to the creation of the Agricultural Division in the Patent Office in 1848, its origins as a federal consumer protection agency began with the passage of the 1906 Pure Food and Drugs Act.” [When and Why Was FDA Formed?](#), U.S. Food & Drug Administration (2018). Software-controlled medical devices and machine learning in clinical diagnostics were obviously not in the initial charter. As traditional software and later machine learning began to play roles in regulated systems, the FDA adapted to address the new regulatory challenges. [Artificial Intelligence and Machine Learning \(AI/ML\)-Enabled Medical Devices](#), U.S. Food & Drug Administration (2021). The FAA has a similar history. When established in 1958, digital avionics were not a factor in regulation

This might require adding AI-specific talent, infrastructure, or training. This will happen only if political leadership prioritizes AI at existing regulatory agencies at the federal, state, and local levels.¹⁴ In addition, the United States needs to develop and use tools and mechanisms to better understand the technical and economic feasibility, including a cost/benefit analysis, of potential regulation.

Third, focus governance on high-consequence use cases. Because it is impractical to govern every AI use or outcome, the United States should shape those AI technologies that will be most impactful. The United States needs a framework for categorizing AI use cases as having the potential to cause major harm, such as widespread discrimination or due process violations. Identifying these types of high-risk AI use cases and enforcing restrictions will require legislative and/or executive actions. There are multiple existing risk characterization frameworks being developed both domestically and internationally that could inform the U.S. national approach.¹⁵

Fourth, strengthen non-regulatory AI governance. In addition to its regulatory guardrails, the United States should strengthen and nurture its robust non-regulatory ecosystem.¹⁶ Civil society participation in governance is an American strength, and non-regulatory mechanisms draw on this by exerting power through incentives and public opinion. Non-regulatory mechanisms can address non-critical AI challenges and harms, and in certain circumstances can be more effective than regulation

Non-regulatory mechanisms can address non-critical AI challenges and harms, and in certain circumstances can be **more effective than regulation in shaping AI development and use.**

and oversight. As the technology advanced and began to play a role in aviation, the FAA adapted and extended its regulatory scope to include digital avionics. [Digital Avionics Systems - Overview of FAA/NASA/Industry-wide Briefing](#), NASA (1986); Emma Helfrich, [DO-178 Continues to Adapt to Emerging Digital Technologies](#), Military Embedded Systems (2021).

¹⁴ Insurance regulation, for example, is largely at the state level in the U.S., and there is a clear focus on what has to be adapted to reflect growing use of AI in the insurance sector. See e.g., Azish Filabi & Sophia Duffy, [State Insurance Legislators at the Forefront of Regulating AI](#), The American College of Financial Services (2022).

¹⁵ Three pre-existing risk characterization frameworks—the [EU AI Act](#) (proposed), European Commission (2021), [AI Risk Management Framework](#) (initial draft), National Institute of Standards and Technology (2022), and [Framework for Classification of AI Systems](#), OECD (2022)—may be useful in providing such guidance on risk-assessment. Each framework takes a slightly different approach, has different goals, and thus yields different implications for how to assess risk.

¹⁶ These include voluntary standards and best practices, self-governance, independent auditing, journalism, advocacy, philanthropy, policy research, legal recourse, government contracting requirements, government funding, incentives, waivers, exemptions, Congressional public hearings and investigations to inform potential legislation, and government-issued policy guidance or frameworks.

in shaping AI development and use.¹⁷ They allow for the flexibility necessary to adjust to a technology that is rapidly evolving and allow for participatory experimentation that can be calibrated and adapted to the maturity of AI. This intentional focus on iterative learning and refinement reflects the reality that any specific mix of AI governance mechanisms is a snapshot in time; technology advances and our understanding of the interactions between AI systems and society must be reflected in our AI governance adaptation. AI and the social environment in which AI is used will continue to change. Governance is ongoing and not an endpoint.

Six Decisive Enablers for Increasing Justified Public Confidence in AI

Public mistrust could dampen adoption of socially beneficial AI-based systems.¹⁸ This mistrust may also encourage an aggressive regulatory stance based on a precautionary, risk-averse approach rather than a more nuanced and informed risk-tradeoff approach.¹⁹ The United States needs a viable public policy reflecting broader consensus in six key areas to help obviate this skepticism in AI and clear the innovation pathway.

- **The United States needs to strengthen privacy protections now while exploring how the proliferation of technology innovations will continue to challenge our society’s conceptions of privacy.**

The creation of data tied to individuals is inherent to our digital world. Data on individuals can be sorted and analyzed to produce inferences about larger groups.²⁰ As part of a larger national data strategy (described in Chapter 2), we need to protect the right to privacy, ensure that networks and services that rely on data are trustworthy and secure, and enable data use and sharing for economic and social good. The United States should prioritize three actions to improve data privacy protections: (1) Pass federal privacy legislation. The collection, combination, and use of data cuts across sectors and thus requires broad federal legislative

17 Non-regulatory mechanisms have traditionally been insufficient to address high risks of harm (e.g., digital avionics and medical devices have consistently been regulated instead of being governed solely by companies).

18 Lee Rainie, et al., [How Americans Think about Artificial Intelligence](#), Pew Research Center (2022).

19 Adam Thierer, [The Proper Governance Default for AI](#), Medium (2022) (“The logic animating the precautionary principle reflects a well-intentioned desire to play it safe in the face of uncertainty. The problem lies in the way this instinct gets translated into law and regulation. Making the precautionary principle the public policy default for any given technology or sector has a strong bearing on how much innovation we can expect to flow from it. When trial-and-error experimentation is preemptively forbidden or discouraged by law, it can limit many of the positive outcomes that typically accompany efforts by people to be creative and entrepreneurial. This can, in turn, give rise to different risks for society in terms of forgone innovation, growth, and corresponding opportunities to improve human welfare in meaningful ways.”).

20 Martin Tisné, [The Data Delusion: Protecting Individual Data Isn’t Enough When the Harm is Collective](#), Stanford Cyber Policy Center (2020).

We need to **protect the right to privacy**, ensure that networks and services that rely on data are trustworthy and secure, and enable data use and sharing for economic and social good.

protections; (2) Prioritize research in privacy enhancing capabilities.²¹ A critical concern is the ability of AI-enabled data fusion and inference to pull sensitive insights from disparate, seemingly innocuous datasets; and (3) Promote sustained public dialogue on the future of privacy. Society's reasonable expectations of privacy are changing as technology advances and our privacy future needs more engagement from all

parts of our society to grapple with difficult questions.²²

- **Facial recognition raises significant concerns that should be addressed through targeted use-case restrictions.**

As with other applications of AI, facial recognition is neither inherently good nor bad, and it is used beneficially in a variety of contexts.²³ Concerns about facial recognition center on privacy and consent, accuracy and bias, and questionable uses and misuses.²⁴ The United States should govern the use of facial recognition technology, not ban the technology.²⁵ There are many positive uses for facial recognition technologies, and polling shows that public support remains significant.²⁶ However,

21 The U.S. Government is already taking important steps to accelerate responses to evolving privacy threats. The Fast Track Action Committee (FTAC) on Advancing Privacy Preserving Data Sharing and Analytics, led by the White House's Office of Science and Technology Policy (OSTP) and the Networking and Information Technology Research and Development (NITRD) Program, is a strong effort to drive advances in the privacy technology space. [Advancing Privacy-Preserving Data Sharing and Analytics](#), NITRD Program (last accessed 2022). The United States and United Kingdom announced they would collaborate on innovation prize challenges for privacy-enhancing technologies. Press Release, [US and UK to Partner on Prize Challenges to Advance Privacy-Enhancing Technologies](#), The White House (2021). The United States and European Union Trade and Technology Council (TTC) also highlighted PETs as a priority area for cooperation. [FACT SHEET: U.S.-EU Trade and Technology Council Establishes Economic and Technology Policies & Initiatives](#), The White House (2022).

22 Karen Hao, [Coronavirus is Forcing a Trade-off Between Privacy and Public Health](#), MIT Technology Review (2020); Derek Korte, [3 Privacy Tradeoffs That Might Be Worth It](#), WIRED (2015).

23 Some examples include unlocking personal mobile devices, accessing ATMs, passing through airport or event security, and checking into hotels. See e.g., [Where is Facial Recognition Used?](#), THALES (last accessed 2022).

24 GAO-20-522, [Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses](#), U.S. Government Accountability Office (2020); Katam Raju Gangarapu, [Ethics of Facial Recognition: Key Issues and Solutions](#), Learn Hub (2022).

25 As an example of a ban, Microsoft is restricting the use of its facial recognition tool and will stop offering automated tools to predict a person's gender, age, and emotional state. James Vincent, [Microsoft to Retire Controversial Facial Recognition Tool that Claims to Identify Emotion](#), The Verge (2022).

26 Lee Rainie, et al., [Public More Likely To See Facial Recognition Use By Police as Good, Rather Than Bad for Society](#), Pew Research Center (2022); Tom Simonite, [Face Recognition Is Being Banned - but It's Still Everywhere](#), WIRED (2021). Even when there is consensus on

without targeted restrictions, this technology risks undermining democratic values, for example, by compromising privacy and exacerbating biases.²⁷ Legal authorities should account for different risk levels and use contexts between the commercial, government, and law enforcement communities.²⁸ The American approach to facial recognition regulations should be sector-specific and enforced by existing sector regulators.

- **We need to increase efforts to operationalize the principle of mitigating unwanted bias in AI.**

One of the strongest motivations for public distrust in AI is its power to amplify existing bias in some cases.²⁹ There is considerable national and global focus on addressing the issue of fairness and bias in AI, highlighted in published AI ethics principles from government, industry, academia, and civil society.³⁰ Despite this attention and investment, there is clearly a long way to go to establish justified confidence in the mitigation of unwanted bias. Progress is needed to: (1) Increase multi-disciplinary focus on ways that AI systems are affected by and affect social constructs, assumptions, and individual and collective behavior.³¹ (2) Implement

a particular use (e.g., combating child exploitation), nuanced challenges remain around how the data was gathered for that application (e.g., via internet scraping of social media). See Richard Van Noorden, [The Ethical Questions That Haunt Facial-Recognition Research](#), *Nature* (2020).

27 Sam duPont, [On Facial Recognition, the U.S. Isn't China - Yet](#), *Lawfare* (2020).

28 A 2021 Center for Strategic and International Studies report proposes a useful set of principles to shape federal rules: Permissible Use, Transparency, Consent and Authorization, Data Retention, Autonomous Use, Redress and Remedy, Oversight and Auditing, Algorithmic Review, and Training Data. See James Lewis, [Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape](#), Center for Strategic and International Studies (2021).

29 [Distrust of Artificial Intelligence: Sources & Responses from Computer Science & Law](#), *Daedalus* (last accessed 2022).

30 AI ethics principles that reference bias include [AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense](#), Defense Innovation Board (2019); [Principles of Professional Ethics for the Intelligence Community](#), Office of the Director of National Intelligence (2014); [Memorandum for the Heads of Executive Departments and Agencies: Guidance for Regulation of Artificial Intelligence Applications](#), Office of Management and Budget (2020); Jessica Fjeld, et al., [Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI](#), Berkman Klein Center (2020); Anan Mahmood, [Tackling Bias in Machine Learning Models](#), IBM (2022); [Responsible AI Practices](#), Google AI (last accessed 2022); Dana Pessach & Erez Shmueli, [A Review on Fairness in Machine Learning](#), ACM Computing Surveys (2022). Efforts to operationalize the principle of mitigating unwanted bias include recommendations from the NSCAI. [Key Considerations for Responsible Development and Fielding of Artificial Intelligence](#), National Security Commission on Artificial Intelligence (2021). The proposed National AI Initiative Act of 2020 requires R&D to mitigate bias. See H.R. 6216, [National AI Initiative Act of 2020](#) (2020). Multiple states have made mitigating unwanted bias a priority. See [Legislation Related to Artificial Intelligence](#), National Conference of State Legislatures (2022).

31 Andrew Selbst, et al., [Fairness and Abstraction in Sociotechnical Systems](#), Conference on Fairness, Accountability, & Transparency (FAT) '19 at 60 (2019) (“[A] sociotechnical frame recognizes explicitly that a machine learning model is part of a sociotechnical system, and that the other components of the system need to be modeled. By moving decisions made by humans and human institutions within the abstraction boundary, fairness of the system can ... be analyzed as an end-to-end property of the sociotechnical frame.”). In an algorithm used to manage the health of populations, it was determined that the disparity was not a problem with bias in the training data or a flaw in the model; it was due to complex societal factors that affect the healthcare interactions of black and white patients in the U.S. that could not be anticipated or understood by looking at the data and model in isolation. See Ziad Obermeyer, et al., [Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations](#), *Science* (2019).

more intentional use of all levers of governance both before and after AI adoption. (3) Increase research and adoption of ways that AI can expose and help mitigate aspects of bias.³² (4) Better understand the ways in which governance of non-AI parts of a system can reduce biases that manifest in the AI system.³³ A specific use of AI may help expose and reduce bias or it may amplify it, but it is often a mirror that reflects the challenges and opportunities in the broader society in which it operates.³⁴

- **AI uses that have a high risk of causing harm require mechanisms for recourse.**

Governing AI outcomes that have a high risk of causing harm requires ensuring that those affected by these AI systems have recourse to learn why they were negatively impacted and ways to address it.³⁵ This would contribute to justified public confidence in AI use by ensuring that people have the option to challenge potentially capricious or erroneous results. It also implies some design constraints on the development of AI that pose a high risk of causing harm. Those adversely affected by AI should have the opportunity to appeal the outcomes of an AI-based system. In many cases, existing regulatory frameworks can be adapted for this purpose.³⁶

- **More timely and effective governance requires capabilities to better explore and understand the complex sociotechnical implications of AI prior to and during use.**³⁷

³² AI also offers a chance to significantly reduce bias and unfairness by making it explicit and correctable over time. Jennifer T. Chayes, [How Machine Learning Advances Will Improve the Fairness of Algorithms](#), Huffington Post (2017).

³³ For example, the mitigation of biases in predictive policing systems is going to require governance of policing practices, not just the AI systems that inform those practices.

³⁴ Rachel Metz, [AI Made These Stunning Images. Here's Why Experts Are Worried](#), CNN Business (2022).

³⁵ [Responsibility, Recourse, and Redress: A Focus on the Three R's of AI Ethics](#), IEEE Technology and Society Magazine at 86 (2022) (“In the context of AI, recourse can be determined as the mechanisms by which a stakeholder (either influencing or impacted) informs responsible persons or organizations of an unexpected, unfair, or unsafe outcome. In the example of a denial of a service or payment, there must be clear guidance identifying the responsible stakeholders, how to contact them, and the right, under relevant regulation, to challenge and ask for reconsideration of the decision process and rectification if an error has been committed.”).

³⁶ As an example of adapting existing regulatory frameworks, current regulations for consumer protections in credit decisions apply regardless of the use of AI in the decision making. [The Equal Credit Opportunity Act requires] “creditors to provide statements of specific reasons to applicants against whom adverse action is taken. The adverse action notice requirements of ECOA , however, apply equally to all credit decisions, regardless of the technology used to make them.” [Consumer Financial Protection Circular 2022-03: Adverse Action Notification Requirements in Connection with Credit Decisions Based on Complex Algorithms](#), Consumer Financial Protection Bureau (2022).

³⁷ “Sociotechnical implications: refers to the implications of AI being embedded in larger “sociotechnical systems,” systems that “consist of a combination of technical and social components.” For example, “fairness and justice are properties of social and legal systems like employment and criminal justice, not properties of the technical tools within.” Andrew Selbst, et al., [Fairness and Abstraction in Sociotechnical Systems](#), Conference on Fairness, Accountability, & Transparency at 59-60 (2019).

Governing emerging technology requires making informed decisions about tradeoffs between priorities. Government and industry lack widespread access to capabilities to explore the interaction of multiple AI systems and human agents that operate together and how the interaction impacts society. The typical reactive approach is to address complex societal effects of an AI system after deployment. We need technical and non-technical capabilities to better anticipate implications of AI on society and the societal influences on these technologies before and during their deployment.

We need technical and non-technical capabilities to **better anticipate implications of AI on society** and the societal influences on these technologies before and during their deployment.

There are emerging tools and techniques that can be used to develop the capabilities to anticipate societal impacts. Modeling techniques are starting to demonstrate the capabilities necessary to explore the complex dynamics of the interaction of multiple AI systems and human agents over time and their effects on the society in which they are introduced.³⁸ The value of these capabilities is not to “predict the future,” but to enable intentional exploration of potential interactions

between an AI system and society to anticipate potential outcomes requiring attention prior to deployment.³⁹

There is urgency to this challenge. AI-enabled decision systems, a critical subset of AI systems, are increasingly used in high-consequence systems. Without better anticipatory capabilities, we will always lag in our ability to mitigate unintended societal harm or we will avoid adopting transformative beneficial capabilities because of reluctance to risk unknown consequences.

- **Social media platforms need a multi-pronged governance approach to address societal harms and mitigate disinformation.**

AI-enabled social media platforms have become part of daily lives, and

38 This is analogous to digital twin techniques, which are currently used to simulate physical objects prior to building them in order to explore design alternatives and implications of a selected design (of jet engines, for example). See Maggie Mae Armstrong, [Cheat sheet: What is Digital Twin?](#), IBM (2020).

39 A recent example of this approach is an agent-based simulation to explore the diffusion and persistence of false rumors in social media networks. See Kai Fischbach, et al., [Agent-Based Modeling in Social Sciences](#), Journal of Business Economics (2021).

dramatically changed our societies. These platforms provide information at an unprecedented volume and scale, revolutionizing how individuals interact. The ability to instantaneously interact with users around the world alters public engagement in an unprecedented way.⁴⁰ But these same platforms destabilize societies and enable the spread of disinformation at a global scale.⁴¹

Multiple elements contribute to the proliferation of disinformation on social media platforms. The harms caused by social media platforms are the result of both business models and user choices.⁴² Therefore, a national strategy to mitigate disinformation should include several components: (1) Direct resources and expertise into developing digital literacy programs for the most affected populations. (2) Develop public trust by working with local news media outlets to bolster dissemination of credible information at the community level and sponsor research into methods for overcoming barriers created by the “Liar’s Dividend.”⁴³ (3) Cooperate with allies and partners, by sharing and learning best practices that could inform U.S. disinformation policy. (4) Find ways to lower toxicity and increase transparency, for example by requiring content publishers to watermark or otherwise label their content with information related to source origin; increase algorithm transparency by varying degrees for users, civil society, and oversight authorities; and allow users to control what type and how much of a certain type of content they see. (5) Continue to develop privacy-protecting tools like unique pseudonyms, which can be useful for detecting and stopping automated bots that propagate disinformation at scale.⁴⁴

40 See generally, José Van Dijck, [The Culture of Connectivity: A Critical History of Social Media](#), Oxford University Press at 3-23 (2013).

41 David M. J. Lazer, et al., [The Science of Fake News](#), *Science* (2018); Sander van der Linden, [Misinformation: Susceptibility, Spread, and Interventions to Immunize the Public](#), *Nature Medicine* (2022).

42 Sara Brown, [The Case for New Social Media Business Models](#), MIT Sloan (2022); Gordon Pennycook & David G. Rand, [The Psychology of Fake News](#), *Trends in Cognitive Sciences* (2021).

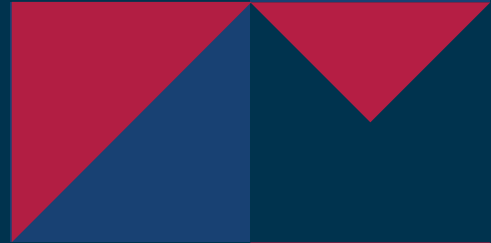
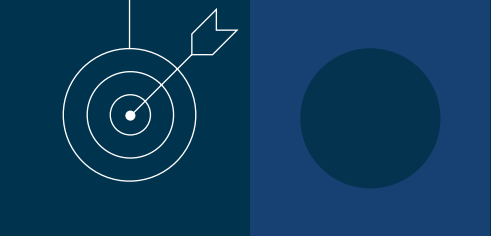
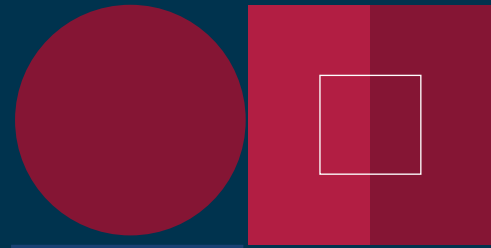
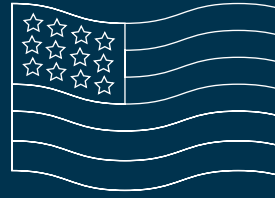
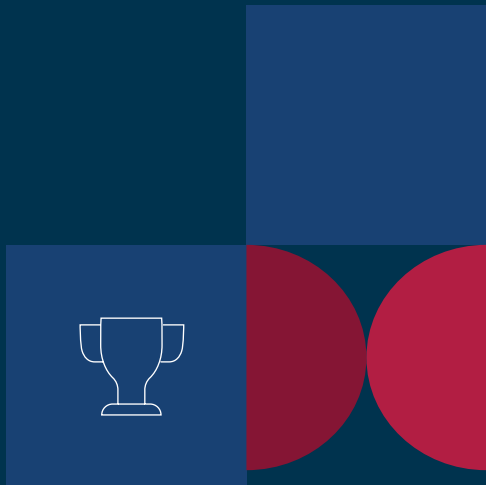
43 The Liar’s Dividend occurs when malignant actors are able to claim valid information as being invalid. It creates an opportunity for malignant actors to potentially further their narratives and objectives by claiming online media is false— which individuals may believe— regardless of the validity of the claim. Robert Chesney & Danielle K. Citron, [Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security](#), *California Law Review* at 1785-86 (2019).

44 The creation of unique pseudonyms online helps identify individual users, while also posing difficulties with connecting an individual online user with the real life person. Pseudonymization is known foremost as a data protection technique, especially for storing data per GDPR standards while protecting personal information. See Thomas Zerdick, [Pseudonymous Data: Processing Personal Data While Mitigating Risks](#), European Data Protection Supervisor (December 2021); see also Lee Rainie, et al., [The Future of Free Speech, Trolls, Anonymity and Fake News Online](#), Pew Research Center (2017).

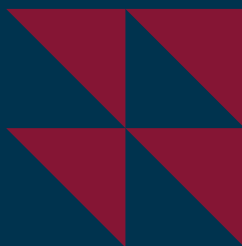
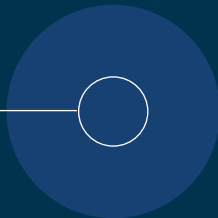
Remaking U.S. Global Leadership in the Age of Technology Competition

Mid-Decade Challenges to National Competitiveness

04



- Transforming U.S. Foreign Policy for the Tech Competition
- Pillar 1: Alliance Resilience and Partnerships
- Pillar 2: Aligning the Private Sector with Strategic Technology Priorities
- Pillar 3: Foreign Policy Organization, Tools, and Workforce: A “Goldwater-Nichols” for Foreign Policy
- Objective 1: Promoting Digital Freedom
- Objective 2: Safeguarding Global Digital Infrastructure
- Objective 3: Engaging the Swing States
- Objective 4: Constructing a New Relationship with China that Reflects Tech Competition
- Next Steps to 2025 and Beyond



CHAPTER 4

Remaking U.S. Global Leadership in the Age of Technology Competition

Technology is now the heart of a long-term, systemic competition between open, democratic societies and closed, authoritarian systems to shape the future of the international rules-based order. In addition to strengthening our techno-industrial foundations at home, the technology competition calls for a broad reexamination of U.S. foreign policy – its objectives, its tools, its organization, and the nature of collaboration with allies and partners.

Technology competition is not simply an economic competition for markets between firms. Technology is power, reach, and influence, and it affects the sovereignty of nations in the digital and physical worlds. Digital infrastructure and tech platforms significantly favor economies of scale, as the network effects from adoption, first-mover advantages, and lock-in effects raise the costs of switching technology platforms and increase the performance of larger networks and platforms.¹ As a result, acting quickly and at scale are almost certainly necessary conditions for foreign policy action in tech competition.

Technology competition is not simply an economic competition for markets between firms. Technology is **power, reach, and influence**, and it affects the sovereignty of nations in the digital and physical worlds.

¹ See John Soroushian, [Digital Platforms Primer: Digital Platforms and Competition](#), Bipartisan Policy Center (2021); Martin Kenney & John Zysman, [The Rise of the Platform Economy](#), Issues in Science and Technology (2016).

A world in which the CCP and firms based in China produce, operate, and control key digital and emerging technologies used by individuals, businesses, and governments will become much less free and open. It puts at risk the security and integrity of the digital world, lowers the barriers to illiberal tech governance and standards,² and ultimately threatens the legitimate sovereignty of nations that rely on technology sourced from authoritarian nations. Instead of a world where nations can expect agreed-upon principles to guide the conduct of international relations, a world order shaped by the PRC's tech sphere of influence would be subject to the whims of the PRC. The result is the single greatest challenge to open democratic societies and a wider world order anchored in the respect for the rule of law.

Yet for much of the world, technology developments are not perceived as part of a strategic contest, and many nations see little distinction between a U.S.-led or PRC-led global order. Their technology choices are made on the basis of national interests and economic calculations. This divergence is the crux of the foreign policy challenge. The United States and its allies will need to offer real technology alternatives to those from the PRC. They must also demonstrate that open societies and the technologies we develop offer greater promise for national success and prosperity than do closed systems and the technologies sourced from authoritarian nations. Doing so will restore faith in a rules-based order

Transforming U.S. Foreign Policy for the Tech Competition

The United States has taken initial steps to meet the moment: reiterating its commitment to Internet freedom, funding digital freedom technologies,³ raising alarm bells about the threat of PRC technologies, promoting U.S. technology exports,⁴ and increasing outreach to partners to build resilient supply chains and coordinate technology policies.⁵ It is time to accelerate these actions to institutionalize the architecture for a long-term competition.

2 Chinese surveillance technology abets authoritarian rule. Chinese apps, too, which operate under different codes of conduct and accountability of most Western firms, provide little if any resistance to takedown requests or other government censorship. See Jeffrey Knockel, et al., [We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus](#), Citizen Lab (2020); Alina Polyakova & Chris Meserole, [Exporting Digital Authoritarianism: The Russian and Chinese Models](#), Brookings at 6 (2019).

3 For example, the U.S. Open Technology Fund received a historic funding increase in 2020 from Congress to support its counter digital authoritarianism work. [OTF's Budget for the 2020 Fiscal Year](#), Open Technology Fund (2020).

4 See e.g., [China and Transformational Exports Program](#), Export-Import Bank of the United States (last accessed 2022).

5 For example, the 2022 Indo-Pacific strategy emphasizes such technology-related partnerships in the region, including through the Indo-Pacific Economic Framework (IPEF). See [Indo-Pacific Strategy of the United States](#), The White House (2022); [FACT SHEET: Indo-Pacific Economic Framework for Prosperity](#), The White House (2022).

Mid-Decade Priorities for Foreign Policy

Four Objectives

- 1 **Promoting** Digital Freedom
- 2 **Safeguarding** Global Digital Infrastructure
- 3 **Extending** Tech Partnerships to the “Swing States”
- 4 **Constructing** a New Relationship with China that Reflects Tech Competition

Three Pillars



Alliance Resilience and Partnerships

1



Aligning the Private Sector with Strategic Technology Priorities

2



Foreign Policy Organization, Tools, and Workforce: A “Goldwater-Nichols” for Foreign Policy

3

We identify *four mid-decade objectives for foreign policy* in the age of technology competition:

- *Promote digital freedom* in an ideologically pluralistic world as the counterweight to closed spheres of digital influence and control, particularly by investing in circumvention technologies that can pierce through firewalls and other forms of authoritarian control, developing a playbook to help manage authoritarian challenges, and supporting civil society globally.
- *Build out resilient, secure, and open global digital infrastructure* to help safeguard data and the next generation of apps and platforms that will drive national security, economic prosperity, and societal cohesion.
- *Strengthen tech partnerships with the “swing states”* – those nations that do not seek to be locked in to either U.S. or PRC technology or ideology – through capacity building and a compelling alliance package of financing, digital infrastructure, apps, and services that reinforces their resilience and sovereignty.
- *Construct a new relationship with the PRC* in a world where technology competition is driving increasing bifurcation and the United States and PRC clash across nearly all fronts.

We recommend three pillars to a U.S. foreign policy strategy to achieve these objectives:

- *Establish alliance partnerships* around technology that leverage allied comparative advantages to compete at scale, reinforce alliance resilience against the authoritarian system, and support enduring alliance technology advantages.
- *Align private sector activity* toward national strategic technology interests within appropriate democratic guardrails and coordinated governance/regulatory frameworks.
- *Structure the United States’ foreign policy organizations, tools, and workforce* to be better fit for tech competition.

The next section elaborates on these pillars and how the United States can leverage these ways and means to organize and lead in the tech competition, followed by discussion and recommendations for achieving the four mid-decade objectives for foreign policy.

Pillar 1: Alliance Resilience and Partnerships

Neither the United States nor any of its allies on their own can compete at scale with the PRC

in the tech competition. The United States and its allies must move beyond coordination and toward institutionalizing alliance techno-industrial cooperation that capitalizes on the benefits of our alliance ecosystem, brings to bear our respective comparative advantages, builds out our collective resilience, and supports democratic leadership. The United States should undertake three priorities to orient our alliances for the tech competition:

- *Globalize alliance coordination by leveling up regional alliance efforts.* We need our alliances to take a global approach to the competition. The United States should leverage its leadership across the Quad, AUKUS, and the U.S.-EU Trade and Technology Council and bring together allies from across the Americas, Europe, and the Indo-Pacific into global partnership.
- *Expand the definition of “winning” — a competition of systems is a team effort with our allies.* Tensions among allies over commercial competition are not new — they are inherent in trade.⁶ However, there should be no question that the United States should prefer to see a company from an allied country win a contract or gain market share in strategic tech sectors where the leading companies may not be American (e.g. 5G networking) — and vice versa — rather than see a PRC company win that contract or gain market share. In areas where the PRC is competitive, the tech competition will require the United States and its allies to balance national commercial interests with alliance resilience, and prioritize commercial partnership over commercial competition.
- *Integrate alliance capabilities and advantages to compete at scale for global markets and to mitigate alliance vulnerabilities.* The PRC brings together “public” and “private” resources, capabilities, and national champions into a package of technology, infrastructure, services, and financing — all with official government backing.⁷ This is essentially a challenge of scale and scope. By working with allies to pool our official resources, the United States can align alliance investments and financing to begin to match the scale of resources the PRC can bring to bear. And by coordinating alliance tech priorities and the comparative advantages our companies have (e.g. one ally may have best-in-class cloud service companies, another may have best-in-class 5G networking), the United States and its allies can facilitate corporate partnerships, such as consortia, that can help deliver compelling global digital infrastructure and other technology solutions that no

⁶ The rivalry between Boeing and Airbus is emblematic, although certainly not the only instance, of intense competition between European states and the United States as strategic allies but economic rivals. John Francis & Alex Pevzner, [Airbus and Boeing: Strengths and Limitations of Strong States](#), *Political Science Quarterly* (2006/7).

⁷ Margaret Pearson, et al., [Party-State Capitalism in China](#), *Current History* (2021).

one nation could muster on its own. Relatedly, the United States and its allies can develop collective alliance resilience by looking first to other allies' companies to fill gaps in capabilities and resources, and thereby mitigate risks of dependencies with the authoritarian system.

Energizing alliance cooperation in the tech competition could include:

- *A small group on next-gen connectivity — United States, Japan, Republic of Korea, Sweden, Finland, EU, and others.*⁸ Even as we work to catch up in the 5G competition, a small group of allies should organize to avoid the mistakes of the past and look over the horizon at next generation network solutions like 6G and space-based systems. The small group can work together to get a headstart on financing, R&D, patents, standards, and production.
- *The “DemTech” Alliance.* Aligning allies' comparative advantages and coordinating complementary regulations, policies, and investments will also be needed — we can do so by building the DemTech alliance of the leading countries in these technologies. Some nations, like Australia⁹ and Canada,¹⁰ already have national technology lists of priorities — aggregation and deconfliction across these lists can be a start. Coordinating democratic leadership in international organizations, like standards setting bodies, can be another initial function.
- *An allied “DemTech Bank.”* The new era of tech competition requires new institutions for the United States and its allies to align our efforts, resources, and values. The PRC recognized this early on and created its Asian Infrastructure Investment Bank to challenge the Washington Consensus.¹¹ A “DemTech Bank” can serve as a counterpoint, pooling allied resources to invest in and support an alliance infrastructure and digital freedom agenda. An initial step could be for allied development finance institutions or export credit agencies to explore co-financing of specific digital infrastructure projects.

Pillar 2: Aligning the Private Sector with Strategic Technology Priorities

Technology companies today manage and secure critical public systems, underpin

8 While the listed countries are home to key companies in this space, core innovations that will define 6G may come from researchers and companies in other countries. We recommend remaining open to engaging with other partner and ally countries with potential in this space, as well as existing international consortia, like the Next G Alliance, that may help in identifying and bringing in other key companies and countries.

9 [Blueprint for Critical Technologies](#), Australian Government (2021).

10 [Key Industrial Capabilities](#), Government of Canada (2021).

11 Daniel C.K. Chow, [Why China Established the Asia Infrastructure Investment Bank](#), Vanderbilt Journal of International Law (2016).

economies by providing the digital scaffolding for other industries' operations, facilitate the flow of information, and serve as global platforms of services. The reach and responsibility of tech platforms now match, and in some cases exceed, those of nation states. Building on the discussion in Chapter 1 of this report on the importance of public-private cooperation for technology advantage, how nations can channel the power of their tech companies is now an essential element of statecraft for geopolitics, for shaping the international order, and in the underlying systemic competition between open societies and closed systems.

The PRC system has a simple approach for incorporating tech power into its statecraft. Central planning and military-civil fusion blur the lines between public and private, leveraging official state support to position its ostensibly "private" tech companies and platforms for global dominance.

The United States and its allies will not win by becoming more like China. Rather, we will need a model for tech statecraft that preserves the independence of our private sectors, which have been central to the dynamism of our tech companies. The United States needs to find a new alignment between government and industry to work toward a shared vision for a democratic future in three key areas:

- *Signal strategic technology interests* where the United States and its allies want to incentivize – or prohibit – private sector investment and activity overseas. For instance, building on the discussion of techno-industrial strategy in Chapter 2 of this report, the United States and its allies need to coordinate and deconflict strategies and policies around the tech sectors where we want greater private sector focus domestically (e.g. semiconductors and subsidies), to maximize the collective return on our investments, and similarly coordinate restrictions on outbound investments in sensitive tech sectors.
- *Establish democratic guardrails* for our private sector's activity at home and abroad, such as around AI governance discussed in Chapter 3 of this report, including on the use of technology and on an approach to data privacy and security that preserves data flows across our ecosystems.
- *Coordinate governance and regulatory frameworks*, building on recommendations in Chapter 2 to develop a national data strategy and in Chapter 3 on AI development,

The United States needs to find a **new alignment between government and industry** to work toward a shared vision for a democratic future...

to ensure the United States, its allies, and our companies can double down on a common ecosystem, standards, and market for tech innovation and development, rather than fracturing them.

Two areas should continue to be prioritized:

- *Double down on U.S. and allied leadership in international technical standards-setting bodies.* Technical standards help determine whether technology develops along a path toward openness and interoperability, or authoritarian-style control. Market-driven and private sector-led tech standards should remain the gold standard. However, more needs to be done at the governmental level to push back against PRC (and to a lesser extent, Russian) attempts to unduly influence outcomes in traditionally-independent expert bodies that would bake top-down control, under the guise of cybersecurity, and restrictions on open data flow into Internet technologies.¹² The United States and allies should continue to promote our leadership in international standards-setting bodies, including by lowering the barriers to participation by U.S.-based researchers and supporting allied candidates for leadership and other key positions.
- *Support the free flow of data for digital trade.* Elements of the U.S.-Mexico-Canada Agreement and the U.S.-Japan Digital Trade Agreement provide a model for the free flow of data as a driver of economic prosperity through greater private sector access across digital markets. This also builds on the “Data Free Flow with Trust” (DFFT) concept championed by the late former Prime Minister of Japan, Shinzo Abe, during Japan’s G20 presidency, whereby DFFT principles would enable cross-border data flows to bolster digital trade and power economic growth.¹³ Efforts against data localization can also bolster the normative digital freedom agenda, a foreign policy objective presented in this chapter.¹⁴

Pillar 3: Foreign Policy Organization, Tools, and Workforce: A “Goldwater-Nichols” for Foreign Policy

The global scale and scope of objectives and strategy for the tech competition require a comprehensive review to align the array of foreign policy authorities, organizations, programming, funding, and talent across the U.S. Government to ensure it is best positioned

¹² For example, technical standards for networks include those protocols adopted by bodies like the ISO, IETF, IEEE, W3C, and ITU. Chinese companies have been increasingly active at both the general membership and leadership levels in these bodies. Daniel Russel & Blake Berger, [Stacking the Deck: China’s Influence in International Technology Standards Setting](#), Asia Society Policy Institute (2021).

¹³ [Data Free Flow with Trust \(DFFT\): Paths towards Free and Trusted Data Flows](#), World Economic Forum White Paper (2020).

¹⁴ Robert Knake, [Weaponizing Digital Trade](#), Council on Foreign Relations (2020).

to win the tech competition. A review should focus on recommend actions — short and long term — in three areas:

- Streamlining the U.S. Government’s foreign policy functions across departments and agencies to minimize duplication;
- Modernizing the programs, roles, and responsibilities within departments and agencies to reflect strategic technology priorities; and
- Recruiting, training, and retaining a tech-forward workforce that can address global technology challenges and reward technology expertise.

Today’s techno-economic competition demands organizational reform. The foreign policy authorities relevant to the tech competition are spread across multiple departments and agencies (e.g., the Departments of State, Treasury, Defense, Energy, and Commerce, the U.S. Agency for International Development, the U.S. International Development Finance Corporation, etc.). Efforts like the creation of the International Development Finance Corporation (DFC) from the Overseas Private Investment Corporation and the launch of the China and Transformational Exports Program (CTEP) at the Export-Import Bank of the United States (EXIM) position these agencies for the tech competition, but more will need to be done to align their modernized missions with the legacy authorities they wield.¹⁵ “Tech” continues to be seen through the lens of “IT support” rather than on par with geopolitical statecraft.¹⁶ Even then, the public sector remains far behind the private sector in adopting cutting-edge technological capabilities at speed and scale.¹⁷ Foreign policy in particular can benefit from data science and analytics and information analysis that tech capabilities offer to support diplomatic tradecraft.¹⁸ And the U.S. Government’s approach to human capital in the foreign policy and national security workforce remains a hurdle for recruiting and retaining talent in the tech space who can advance the priorities of tech competition.¹⁹

As discussed in Chapter 1 of this report, the creation of the National Economic Council

¹⁵ [U.S. International Development Finance Corporation, Management Challenges Facing the U.S. International Development Finance Corporation in FY 2022](#), Office of the Inspector General (2021); Daniel F. Runde & Alexander Mayer, [Moving Forward: an Ex-Im Bank for the Twenty-First Century](#), Center for Strategic and International Studies (2021).

¹⁶ One example is the U.S. Department of State’s Foreign Affairs IT Fellowship, which while an important career pathway for information management specialists, is discussed as a flagship program for attracting “technology talent” to the Department. [About](#), Foreign Affairs IT Fellowship (last accessed 2022).

¹⁷ [Secretary of Defense Austin Remarks at the 2021 Global Emerging Technology Summit of The National Security Commission on Artificial Intelligence](#), U.S. Department of Defense (2021).

¹⁸ [Less Art, More Science: Transforming U.S. Foreign Policy Through Evidence, Integrity and Innovation](#), FP21 (2020).

¹⁹ See [Final Report](#), National Security Commission on Artificial Intelligence at 119 (2021).

..the digital infrastructure race, or bleak trendlines for global digital freedom, should be the wake-up call that **the U.S. needs a “Goldwater-Nichols” for foreign policy** in the era of tech competition.

and the National Security Council are examples of leadership and foresight in positioning the U.S. Government for a new era of competition. Other broad-ranging functions of government have reorganized after events revealed their deficiencies.²⁰ Perhaps the digital infrastructure race, or bleak trendlines for global digital freedom,²¹ should be the wake-up call that the United States needs a “Goldwater-Nichols” for foreign policy in the era of tech competition.

The United States should act before it is too late.

The analogy of jointness that “Goldwater-Nichols” offers is important given that technology is a “substrate that cuts across every aspect of our foreign policy.”²² Any foreign policy reform or reorganization should prioritize modernizing and streamlining duplicative roles and responsibilities across departments and agencies, alongside building the appropriate interagency architecture (e.g., the proposed Technology Competitiveness Council) to coordinate implementation of tech strategy. Equally important should be requirements around “joint” assignments to ensure foreign policy officials have exposure to the array of roles and responsibilities the U.S. Government has with respect to tech policy, and training requirements to build tech literacy and competencies across the foreign policy workforce.

Beyond a review of what a “Goldwater-Nichols” for foreign policy would look like, near-term recommendations to bridge the gap and elevate tech in foreign policy include:

- *Establish an Office of Technology Transition Initiatives.* Following the dissolution of the Soviet Union,²³ the United States deployed experts to help transitioning nations’ reform efforts and consolidate the nuclear weapons stockpile of the former Soviet Union. The United States government needs to again be able to deploy overseas

20 See, e.g., Pub. L. 99-433, [Goldwater-Nichols Department of Defense Reorganization Act](#) (1986); Pub. L. 108-458, [Intelligence Reform and Terrorism Prevention Act](#) (2004).

21 [Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet](#), Council on Foreign Relations (2022).

22 See Suzanne Smalley, [State Department Needs More Cyber Policy Muscle, Says Cyberspace Ambassador Nominee](#), Cyberscoop (2022) (quoting Ambassador at Large for Cyberspace and Digital Policy-designate Nate Fick’s nomination hearing testimony).

23 John V. Parachini, et al., [Diversion of Nuclear, Biological, and Chemical Weapons Expertise from the Former Soviet Union: Understanding an Evolving Problem](#), RAND Corporation (2005).

a cadre of experts, this time in tech, to advise partner governments on network infrastructure, cybersecurity, and digital freedom. Following the model of the U.S. Agency for International Development (USAID's) Office of Transition Initiatives, an Office of Technology Transition Initiatives can be created in the Department of State or USAID with authorities to hire and deploy technical talent on overseas assignments.

- *Establish a Peace Corps for tech – a Global Tech Corps.* While Peace Corps has some programs around science, technology, engineering, and mathematics (STEM),²⁴ a more dedicated Global Tech Corps can send volunteers around the world to help build digital literacy and other STEM competencies in lower income countries. There will be practical challenges for such a mission, but opportunities will exist for Americans to fill gaps in capacity building overseas in technology that support our national interests.
- *Increase training, build STEM policy literacy, and create more tech officer positions in the Department of State.* The NSCAI also made recommendations along these lines.²⁵ For example, the Department of State offers some technology training modules and academic or fellowship opportunities to build STEM knowledge and experience,²⁶ but more training should be available and required for more officers to strengthen their tech policy expertise in diplomatic tradecraft. Building on the creation of a new Bureau of Cyberspace and Digital Policy, which elevated technology's importance at the State Department,²⁷ a new dedicated technology officer professional track²⁸ can build the bureaucratic infrastructure necessary to incentivize technology career paths.

Objective 1: Promoting Digital Freedom

The future of the Internet is up for grabs. The PRC, Russia, and others are building a new digital Iron Curtain of “splinternets” and promoting their model abroad.²⁹ Many nations,

24 Peace Corps Response, [7 Unique STEM Positions You Can Apply to Right Now](#), Peace Corps (2018).

25 [Final Report](#), National Security Commission on Artificial Intelligence at 241 (2021).

26 See [Fellowships – Office of the Science and Technology Adviser](#), State Department (last accessed 2022).

27 [Establishment of the Bureau of Cyberspace and Digital Policy](#), State Department (2022).

28 Foreign Service Officer (FSO) generalists choose between five specialties or “cones:” economics, political, consular affairs, management, and public diplomacy. Adding a technology cone, or track within existing cones (more policy-focused than Information Resource Management specialists) would allow FSOs to build their specialties around emerging technologies.

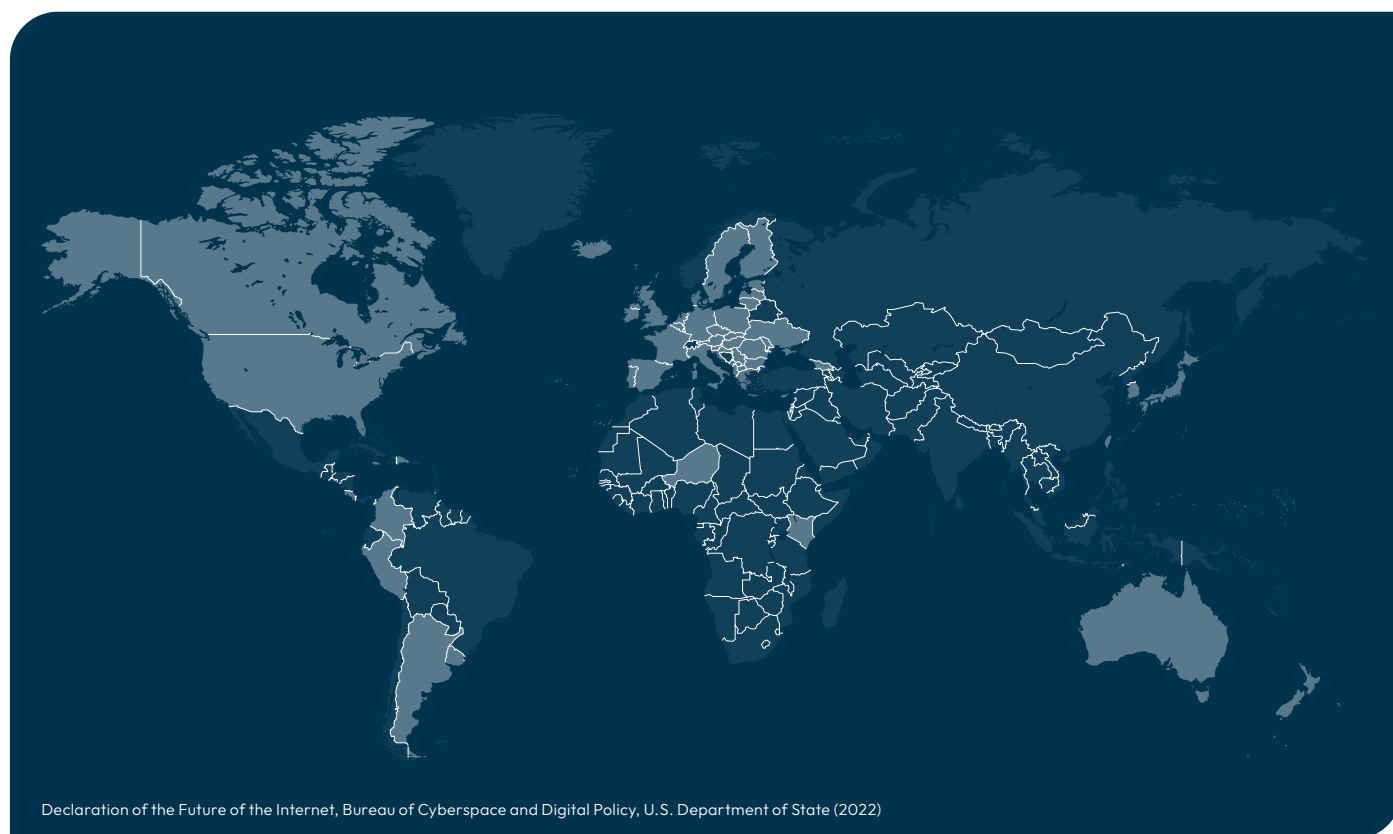
29 Each nation has a slightly different approach to establishing “Internet sovereignty,” but co-option of service providers or Internet infrastructure that is otherwise universal is a common feature. [Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet](#), Council on Foreign Relations (2022).

including democracies and U.S. allies, are being seduced by aspects of closed systems that prioritize surveillance, censorship, and government control of the digital world.

- *Build the norms of acceptable practices.* The world needs clear baselines for acceptable behavior online in the digital age. The United States and its partners have affirmed that the Internet’s north star remains openness. In the recently launched Declaration for the Future of the Internet (DFI), more than 60 countries signed on to support a digital world that is “open, free, global, interoperable, reliable, and secure.”³⁰ More will need to be done with this type of normative baselining in areas such as freedom of expression online. Nevertheless, such baselining can help shape the decisions nations and companies take as they develop, purchase, and apply emerging technologies.

³⁰ [Declaration for the Future of the Internet](#), U.S. Department of State (2022).

The Declaration for the Future of the Internet



- | | | |
|-------------------------|----------------------|------------------------------|
| 1. Albania | 22. Germany | 43. New Zealand |
| 2. Andorra | 23. Greece | 44. Niger |
| 3. Argentina | 24. Hungary | 45. North Macedonia |
| 4. Australia | 25. Iceland | 46. Palau |
| 5. Austria | 26. Ireland | 47. Peru |
| 6. Belgium | 27. Israel | 48. Poland |
| 7. Bulgaria | 28. Italy | 49. Portugal |
| 8. Cabo Verde | 29. Jamaica | 50. Republic of Korea |
| 9. Canada | 30. Japan | 51. Romania |
| 10. Colombia | 31. Kenya | 52. Serbia |
| 11. Costa Rica | 32. Kosovo | 53. Slovakia |
| 12. Croatia | 33. Latvia | 54. Slovenia |
| 13. Cyprus | 34. Lithuania | 55. Spain |
| 14. Czech Republic | 35. Luxembourg | 56. Sweden |
| 15. Denmark | 36. Maldives | 57. Taiwan |
| 16. Dominican Republic | 37. Malta | 58. Trinidad and Tobago |
| 17. Estonia | 38. Marshall Islands | 59. United States of America |
| 18. European Commission | 39. Micronesia | 60. United Kingdom |
| 19. Finland | 40. Moldova | 61. Ukraine |
| 20. France | 41. Montenegro | 62. Uruguay |
| 21. Georgia | 42. Netherlands | |

- *Develop a playbook between governments and the private sector on doing business in authoritarian states.* A lesson learned from the tech sector’s reactions to Russia’s invasion of Ukraine — including how to navigate tensions between withdrawing services and maintaining connectivity — is to form a common public-private approach for dealing with challenges in authoritarian contexts. The United States and allied governments should participate in multi-stakeholder dialogue with tech firms and civil society groups to develop a playbook - triggers and possible responses - to dealing with pressure from other authoritarian regimes and growing repressive activities elsewhere.
- *Invest in, and support, the technological front to reinvigorate digital freedom.* The United States should cooperate with allies and the private sector to harness the wave of emerging technologies that hold promise for enhancing privacy, circumventing censorship, and overcoming Internet shutdowns.³¹ Areas to explore include new privacy-centric technologies,³² better virtual private networks (VPNs), and mesh networks and other decentralized solutions for connectivity.³³ Here, the United States and its allies should also use diplomacy to prevent governments from targeting U.S. (and other democratic) platforms through undue restrictions on market access or intimidation.
- *Double down on civil society around the world.* Foreign assistance and capacity building on digital freedom must prioritize actors who best understand the situation and environment on the ground, i.e., civil society groups operating in their own countries. Investing in their development and building relationships remain essential when it comes to shaping the digital freedom environment.

Objective 2: Safeguarding Global Digital Infrastructure

Digital infrastructure such as wireless networks (especially 5G and its successors), fiber-optic cables (both terrestrial and undersea), operating systems, and servers (cloud and physical) are the foundations upon which digital economies and other technologies function. Control over digital infrastructure confers influence over the data, applications, and platforms of the technology stack. In the hands of authoritarian nations this control

31 See Pak Yiu, [Hong Kong's Apple Daily to Live on in Blockchain, Free of Censors](#), Reuters (2021); Orson Lucas, [Privacy Technology: What's Next?](#), KPMG (2021); [The Future of Decentralized Wireless – Opportunities from 3G Shutdowns and 5G Alternatives](#), RCR Wireless News (2022).

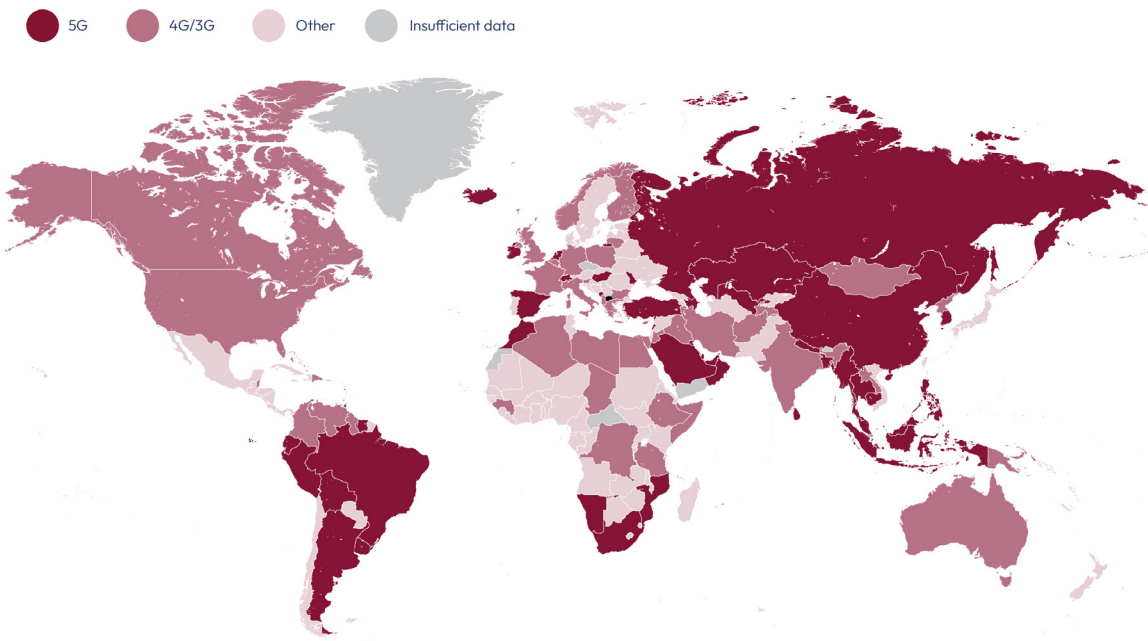
32 See e.g., Alexandra Wood, et al., [Differential Privacy: A Primer for a Non-Technical Audience](#), Vanderbilt Journal of Entertainment & Technology Law (2018); [Zero-Knowledge Proofs](#), Binance Academy (last accessed 2022).

33 See e.g., [Helium](#) (last accessed 2022); [What is IPFS?](#), IPFS (last accessed 2022); [Welcome to the Permaweb](#), The Arweave Project (2019).

becomes coercive political leverage, putting power over information flows into the hands of unaccountable firms responsive to autocrats rather than the rule of law, and creating a technology dependency, similar to energy dependence today, that undermines nations' economic freedom of action. As a result, the PRC's pervasive global footprint in digital infrastructure sectors creates security, economic, ideological, and sovereignty challenges for nations that rely on its technology. Its Digital Silk Road (DSR) offers an appealing bundle of technology that includes 5G, end-to-end connectivity, cloud services, payments architecture, and surveillance solutions.³⁴ At least 16 countries have signed official memorandums of understanding (MOUs) with the PRC authorizing DSR cooperation, and dozens are using PRC digital infrastructure.³⁵

Huawei & ZTE Telecom Presence

PRC telecommunications companies Huawei and ZTE have expanded their reach across the globe.



Note: "5G" indicates Huawei or ZTE 5G networks or technology is either already in use or planning to be used. "4G/3G" indicates Huawei or ZTE has built either 4G or 3G networks. "Other" includes other relationships with Huawei or ZTE, including telecom equipment sales, data centers, smart cities, investments, overseas offices, research partnerships, R&D labs, talent exchanges, fiber-optic cables, subsidiaries, surveillance equipment sales, and training.

Source: SCSP analysis of publicly available information and databases.

34 Eva Dou, [Documents Link Huawei to China's Surveillance Program](#), Washington Post (2021); Jonathan Hillman & Maesea McCalpin, [Huawei's Global Cloud Strategy](#), Center for Strategic and International Studies (2021).

35 [Assessing China's Digital Silk Road Initiative](#), Council on Foreign Relations (last accessed 2022).

The United States and its allies must support and build resilient, secure, and open global digital infrastructure. Competing at scale against the PRC in these tech sectors will require new mechanisms of alignment across allied governments and the private sector, such as coordinated commercial promotion, pooled financing, and concerted funding for new, alternative technologies.

- Tools, tactics, and goals will need to be calibrated across the different digital infrastructure sectors, depending on the local environment, market, and challenges facing U.S. companies.
- We will need deeper engagement with swing state partners so the United States and its allies can better provide the fit-for-purpose technology bundles (e.g. infrastructure, services, apps) that address practical problems, build partner capacities for governance and economic development, and ultimately create new markets and greater opportunities for cooperation on the basis of respect for principles of openness and interoperability.³⁶
- Heavy U.S. diplomatic attention on 5G networks should expand to account for the fact that PRC's DSR packages often include a full suite of hardware, services, financing, and other incentives. To better compete against the PRC's tech packages, we will need an integrated approach around commercial promotion for the export of the full ecosystem of infrastructure, alongside financing, apps, and services. In many areas including cloud services, U.S. companies hold considerable advantages.

Additional actions the United States can take to better compete for global digital infrastructure include:

- *Create a "Global Technology Accelerator Center."* A centralized Center, in either the Department of State or Commerce or as a standalone agency, could align responsibilities and people to identify commercial opportunities abroad in digital infrastructure and other technologies. The Center could help structure U.S. or alliance bids for contracts, in partnership with private sector companies, and mobilize financing, commercial promotion, and diplomatic advocacy across the U.S. Government to win deals.
- *Expand EXIM's and DFC's authorities to finance digital infrastructure deals.* As the NSCAI also recommended, expanded authorities for commercial promotion and development finance could allow the United States to better compete abroad for

³⁶ Tech solutions should not be overly generic and should instead adapt to needs and existing tech capacity in recipient countries. For example, it could be that space-based networks are more useful than 5G to less-populated countries.

digital infrastructure deals.³⁷ Options can include concessional funding, redefining “made in America”³⁸ to better capture U.S. intellectual property used in allied technology, and enabling U.S. agencies to operate globally, including in higher-income countries.

- *Build out digital public goods.* Digital public goods (DPGs) and digital public infrastructure (DPI), which rely on open source software, data, models, standards, and content for e-governance and other commercial or consumer uses, offer a novel approach for the United States and allies to cooperate in developing digital solutions for local and national governance at scale and at low cost³⁹ that can be tailored to partners’ needs. This can help create openings for companies from allied countries to provide downstream digital goods and services, particularly in nations where the United States and its allies may not currently be competitive. DPGs’ and DPI’s open source architecture may also help advance the digital freedom agenda.⁴⁰

Objective 3: Engaging the Swing States

Most nations do not seek to be locked in to either U.S. or Chinese technology or ideology. They want low-cost effective technology, and they want to preserve their sovereignty and freedom of action amidst the great power competition. Their choices, however, could tip the scales in the competition.

Engaging swing states requires getting back to diplomatic basics. The United States will need to better tailor its messaging to and engagement with these partners on where our interests converge. The United States will need to explain the new era of tech competition, the new challenges and opportunities that abound, the authoritarian threats to the sovereignty of nations that we face in common, and the value of the technology packages we can offer. Certain nations will be obvious priorities for alliance engagement given the size of their market, their geographic importance, or key resources they provide in the tech competition. However, the global nature of both the competition and networked systems means that the United States will also need an alliance full-court press for positional

37 See [Final Report](#), National Security Commission on Artificial Intelligence at 241 (2021).

38 “Made in America” requires 55% of a product to be made domestically. See [Fact Sheet: Biden-Harris Administration Issues Proposed Buy American Rule, Advancing the President’s Commitment to Ensuring the Future of America is Made in America by All of America’s Workers](#), The White House (2021). In March 2022, the FAR Council published a [final rule](#) implementing changes that will increase the content threshold requirement immediately to 60% and 75% over the next several years. This rule will go into effect on October 25, 2022.

39 See [Digital Public Goods Alliance: 5 Year Strategy 2021-2026](#), Digital Public Goods Alliance (2021); [Software Global Goods: A Valuation Framework](#), United States Agency for International Development (2019).

40 [Setting a Standard for Digital Public Goods](#), Digital Public Goods Alliance (2020).

advantage everywhere by:

- *Building a common understanding of how technology and systemic competition are challenging the sovereignty of nations.* The nature of the global tech competition, the implications of digital dependence and the importance of digital resilience, remains poorly understood around the world. This is a story that needs to be told in private and in public through capacity building to help partners understand the risks and where the United States and its allies can help provide resilience.
- *Exposing the fiction behind the PRC's Tech Offerings.* The PRC's promise of "common development"⁴¹ and common prosperity⁴² underdelivers and exposes its partners to security risks. In addition to the threats regarding digital dependence, regular reports of Belt and Road Initiative and DSR projects being delayed or over-budget and facilitating espionage raise questions about China's ability to deliver on its commitments and its intentions. All of these are opportunities to expose the fiction of what China is selling and tee up practical alternatives that the United States and its allies can offer.

41 Jennifer Staats, [Four Takeaways from China's Tour of the Pacific Islands](#), United States Institute of Peace (2022).

42 Ryan Hass, [Assessing China's "Common Prosperity" Campaign](#), Brookings (2021).

The Fiction Behind Common Development

Multiple examples highlight that the PRC's digital infrastructure projects may overpromise and underdeliver on cost, speed, and security.

Australia - 2012

- Huawei software update loaded malicious code onto network that siphoned data into China
- Officials confirmed Chinese spy services were behind the breach

Source: Jordan Robertson & Jamie Tarabay, Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack, Bloomberg (2021).

Ethiopia (African Union) - 2017

- IT workers discovered that data was being transferred nightly from the AU Headquarters, which was built by Chinese companies, to servers in Shanghai
- AU was forced to remove and replace all Chinese hardware at its own expense
- Separately, hidden surveillance equipment suspected to have come from the PRC was also found in AU Headquarters

Source: China's Digital Colonialism, Recorded Future (2021).

Papua New Guinea - 2018

- Numerous security vulnerabilities were discovered in a Huawei data center built for the government
- Firewall gaps and outdated encryption were built-in by design
- The \$53 million system went largely unused by government departments

Source: China's Digital Colonialism, Recorded Future (2021).

Ecuador - 2011

- Huawei helped build a national surveillance system as part of a \$19 billion China-Ecuador infrastructure partnership
- The government is paying for the expensive equipment in part by signing away oil reserves – over 80% of Ecuador's oil exports are flagged for China
- Community leaders and citizens have found the system ineffective in slowing crime

Source: Nicholas Casey & Clifford Krauss, It Doesn't Matter if Ecuador Can Afford This Dam, China Still Gets Paid, New York Times (2018). China's Digital Colonialism, Recorded Future (2021).

Pakistan - 2016

- Islamabad's \$100 million Huawei safe city system has proven ineffective, with a 33% increase in crime
- Delays and cost overruns have plagued major infrastructure projects, such as undersea cables meant to connect China, Pakistan, and Africa. Pakistan's repayment obligations stand at over \$40 billion.

Source: Jonathan Hillman & Maesea McColpin, The China-Pakistan Economic Corridor at Five, CSIS (2020). Huawei's Claims that it Makes Cities Safer Mostly Look Like Hype, Bloomberg (2019).

Egypt - 2019

- A major announced 5G network partnership planned for completion by 2020 has yet to materialize
- This is one of several similar failures, including opaque negotiations over a renovated capital city, that foundered suddenly and inexplicably

Source: Allison McManus, Egypt and China's Telecoms: A Concerning Courtship, National Endowment for Democracy (2020).

- *Toning down the rhetoric around “democracy” and values in the tech competition, and instead put our money where our mouth is.* Politically, the colonial legacy of the global north in the global south taints the rhetoric around freedom. Economically, China is the leading trade partner for many nations around the world and “common development” resonates better — rhetorically at least — in some areas of the world than does Western-style “democracy.” The United States and our allies cannot rely on rhetoric to win over partners with good intentions. We need to compete and coordinate on practical alternatives and explain how our technology solutions better address swing state interests in their own resilience and sovereignty.
- *Maintaining the open door and increasing people-to-people connections.* As noted in the discussion on immigration in Chapter 2 of this report, a key strength for the United States and its allies is the openness and diversity of our societies. We want a diversity of students, scientists, entrepreneurs, and others to continue forming the fabric of a prosperous, diverse, and secure America, regardless of national origin. The United States and its allies will not win the tech competition if we cannot foster sustainable relations with the next generation of innovators and leaders around the world. We should expand, by an order of magnitude, leadership and tech talent exchanges with the swing states, in partnership with allies and the private sector. The United States should also partner with allies to develop joint STEM programming and scholarships to identify, train, and bring untapped talent from the swing states into a global tech workforce.

Objective 4: Constructing a New Relationship with China that Reflects Tech Competition

Defining the acceptable bounds of a technology relationship with the PRC and preserving stability in relations will be central challenges for the United States and its allies. As the United States arrives at a new consensus on what the bounds of a new relationship look like, the most challenging issue for the future may be maintaining predictability and stability in the U.S.-China relationship as they become increasingly disconnected technologically and economically. Both the United States and the PRC are seeking to reduce the linkages between their tech ecosystems, particularly in strategic sectors. The United States⁴³ and some allies, such as Australia,⁴⁴ Canada,⁴⁵ and the UK,⁴⁶ have taken steps to cut ties to PRC entities that pose national security risks and violate human rights. The PRC has prioritized

43 [Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China](#), The White House (2021).

44 Jamie Smyth, [Australia banned Huawei over risks to key infrastructure](#), Financial Times (2019).

45 David Ljunggren & Steve Scherer, [Canada to Ban Huawei/ZTE 5G Equipment, Joining Five Eyes Allies](#), Reuters (2022).

46 [Huawei ban: UK to Impose Early End to Use of New 5G Kit](#), BBC News (2020).

..the most challenging issue for the future may be **maintaining predictability and stability in the U.S.-China relationship** as they become increasingly disconnected technologically and economically.

developing its domestic tech industry in order to insulate its economy from external dependencies.⁴⁷ Both sides are trying to protect strengths and compensate for weaknesses in their tech ecosystems with no end of the larger strategic rivalry in sight.

- *Clearly scoping and prioritizing the key areas where the United States wants to reduce or sever tech linkages with China will be essential for the future trajectory of both the bilateral relationship and*

shape how the United States rallies its allies. The U.S. Government will need to clearly delineate - in coordination with allies - the tech sectors where PRC involvement poses the greatest risk and is not acceptable. This will enable more consistent and cohesive technology policies, provide clarity on how the United States, its allies, and our private sectors engage with the PRC, and, building on the discussion in Chapter 2, create clear areas where alliance cooperation and investment can deepen techno-industrial collaboration to strengthen our shared resilience and diversify tech supply chains across the alliance.

- *Dialogue between the two great powers will be even more important to mitigate the risks and consequences of miscalculation and preserve stability in the international order in the midst of competition.* Deconfliction mechanisms, like hotlines between capitals and communications between chiefs of defense, already exist between the United States and the PRC. Dialogues between the two sides have not yet been productive in delineating the bounds of this new competition. China has used them for political gain. This should not be a surprise. It took years and decades to develop the various multilateral and bilateral treaties on nuclear non-proliferation, testing, and arms limitations and reductions in the Cold War. Negotiations were regularly used for broader diplomatic objectives. In the future, dialogue will remain necessary as a means to ensure clarity for both systems on the rules and red lines of the competition.

⁴⁷ Translation, [Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035](#), Center for Security and Emerging Technology (2021).

- *Prioritize people-to-people engagements with Chinese citizens as a positive connection between our two nations.* Millions have immigrated from China to the United States and helped build the U.S. economy,⁴⁸ and hundreds of thousands, if not millions, of American and Chinese students have participated in educational exchanges to both countries,⁴⁹ helping build a better understanding of each other's countries. All of these are beneficial to our nation. Even as we compete against authoritarian regimes, we have to remember to distinguish between the states and their people. We should welcome those who subscribe to our values.

Next Steps to 2025 and Beyond

The alliance approach outlined in this chapter is applicable to competing in any technology sector, and also frames the cooperation the United States can build to advance its priorities in the following chapters on defense and intelligence. Beyond microelectronics, 5G, and AI, the United States and its allies will need to build a common understanding around the challenges and opportunities in biotechnology, quantum computing, future energy systems, and other emerging technologies that are discussed in Chapter 7 of this report. The United States and its allies will need to provide a vision for what a democratic, technology-enabled future looks like in practice and how open societies can use them to offer security, prosperity, sovereignty, and freedom. And we must organize a DemTech Alliance of leading democracies, as well as civil society and private sector partners, that will conduct the research, develop the institutions, build the technologies, and guide their responsible uses to bring about this vision.

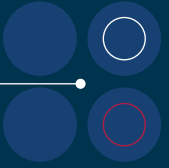
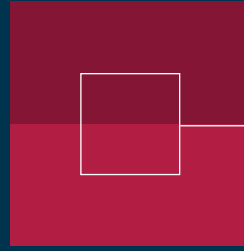
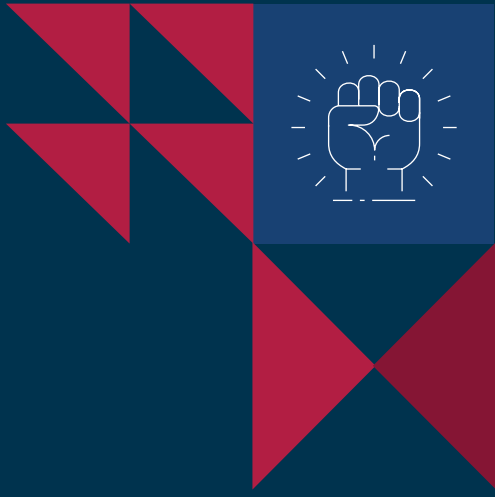
⁴⁸ [China Immigration Statistics 1960-2022](#), Macrotrends (last accessed 2022).

⁴⁹ [Educational Exchange between the United States and China](#), IIE (2008).

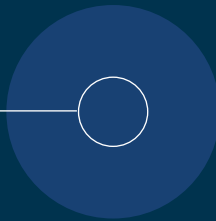
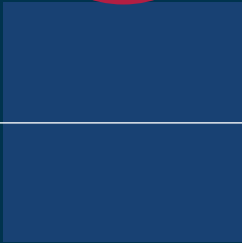
The Future of Conflict and the New Requirements of Defense

Mid-Decade Challenges to National Competitiveness

05



- Changing Conflict and Warfare
- The People's Liberation Army's Theory of Victory to Defeat the U.S. Military
- United States' Asymmetric Strengths that Offer Opportunities for Advantages
- From Asymmetries to Advantages: An Offset-X Strategy



CHAPTER 5

The Future of Conflict and the New Requirements of Defense

The character of war is changing. Before the end of this decade, the United States and its allies will face a new kind of warfare. Advanced and emerging technologies, including artificial intelligence, combined with operational concepts that harness them in innovative and unexpected ways, are creating new ways to apply military force. America's principal rival, China, is harnessing these changes with the aim of eroding or even leapfrogging the United States' military strengths. Meanwhile, the brittleness of America's defense industrial base, the slow transition in U.S. military capabilities from a small number of exquisite legacy systems to many lower-cost, innovative systems, and the struggle to shift from traditional operational concepts compound these challenges. The stakes could not be higher. If the United States does not rise to this challenge, the consequences could be dire: a shift in the balance of power globally, and a direct threat to peace and stability that the United States has underwritten for nearly 80 years in the Indo-Pacific – the most economically, technologically, and resource-critical region of this century.

The United States should respond neither with despair nor hubris. Throughout history, the American military has demonstrated an ability to employ military capabilities in new and innovative ways to confound adversaries. Moreover, the United States retains significant military-technological advantages that it can continue to leverage. Where our military overmatch has been compromised, we can rebuild it. Where our self-confidence has been shaken, we can regain it. But it will require decisive action now to reverse the ongoing erosion of U.S. military advantage.

This chapter outlines a technology-centered strategic approach the United States should pursue to begin accomplishing this. We start by describing how the character of conflict

has changed and is expected to change over the next several years and what the U.S. military — and the country — must do to prepare for the coming changes. We explain how China aspires to defeat the United States in conflict. We then identify existing U.S. military-technological strengths that can be leveraged to create advantages that will be difficult for China to quickly duplicate. We conclude by outlining a new approach — what we term an Offset-X¹ strategy — that could begin to lay the groundwork for the United States to circumvent China’s military advancements and thwart its theories of victory, restore America’s ability to more freely project power in the Indo-Pacific region, and position the United States to honor its commitments to the stability of the region.

We contend that by pursuing the **Offset-X strategy**, which should form the framework for the next National Defense Authorization Act, the U.S. military would be better prepared and positioned to outsmart, outpace, outmaneuver, and — as necessary — outgun the People’s Liberation Army.

The approach we propose can achieve these aims by pursuing primacy in situational awareness, by optimizing the collaboration and teaming between the United States’ highly trained servicemembers and machines, by turning China’s wide geographical exposure and oppressive domestic political control into an American advantage, by creating better software and the ability to adapt it more quickly, and by further empowering leaders at the lowest tactical levels. We contend that by pursuing the Offset-X strategy, which should form the framework for the

next National Defense Authorization Act, the U.S. military would be better prepared and positioned to outsmart, outpace, outmaneuver, and — as necessary — outgun the People’s Liberation Army.

Changing Conflict and Warfare

New military capabilities, their novel application, and intensifying geopolitical rivalry are changing the very character of war and peace. We already see the emergence of this changing character in Ukraine. This new type of warfare will be shaped by both strategic

¹ We refer to the proposed strategic approach as Offset-X to draw an analogy with the [past three Offset strategies](#) that the United States military pursued from 1950 to 2017 with great results. We chose to use X rather than Fourth Offset to ensure that our proposed actions are viewed as only a partial, not a comprehensive list of actions and whose attainment should be viewed as a temporary achievement that needs further revisions and updating.

and operational developments.

At the more *strategic* level, we see the following dynamics:

- *Persistent conflict below the level of armed clashes.* Repeated acts of aggression by authoritarian governments in China (and Russia), often enabled by advanced and emerging technologies, blur the lines between war and peace. These actions include frequent cyber-attacks, unrelenting disinformation operations, aggressive theft of intellectual property, and sabotage.² Even if most of these actions are invisible to many Americans, they leave little doubt that the United States is now in a state of persistent *conflict* with Russia and China.
- *The likelihood of war between great powers is rising.* The blurring of lines between war and peace, acts of aggression by China and Russia, and the high stakes involved increase the risk of major war for the United States. Such a war would be unlike anything Americans have experienced. In the minds of many contemporary Americans, war has been something that happens elsewhere, with American forces experiencing relatively fewer casualties compared to past conflicts. Today's technology changes that. The United States faces the growing threat of large-scale cyber-attacks on the homeland that could paralyze society, the disablement or destruction of space-based assets that underpin the economy and military operations, and even missile strikes on U.S. soil.
- *Great power wars have the potential to devolve into protracted contests that place a high premium on the strength of the industrial base, innovation ecosystem, and political will.* Knockout blows, decapitation strikes, and decisive battles rarely materialize in wars between great powers. Instead, great power adversaries are able to mobilize populations and resources in ways that cause wars to descend into long, grinding contests, in which political will and national resources play as large (or larger) a role as brilliant operational maneuver and deception. However, most Western economies – the United States included – lack the industrial capacity

...the United States is now in a state of persistent **conflict** with Russia and China.

² [Gray Zone Project](#), Center for Strategic and International Studies (last accessed 2022); [China Cyber Threat Overview and Advisories](#), Cybersecurity & Infrastructure Security Agency (last accessed 2022); David Bandurski, [China and Russia are Joining Forces to Spread Disinformation](#), Brookings TechStream (2022).

to rapidly replenish and sustain their forces. This includes the production of the necessary munitions, sensors, vessels, vehicles, and aircraft, possibly for months or even years into a conflict, as well as skilled personnel to produce them. The brittleness of the defense industry can become a serious strategic liability for the United States, presenting U.S. decision-makers with a tough dilemma of whether to escalate vertically or opt out of a conflict.

In addition to the resilience of the industrial base, the vibrancy and responsiveness of the innovation ecosystem to conflict requirements will also be key in a potential great power war of protracted nature. Quickly identifying, repurposing, and fielding new technologies and platforms could shift the tactical tide of war and prove to be of strategic importance. Finally, the industrial base and the innovation ecosystem, while necessary, are not sufficient. They are no substitute for political will to endure and persevere in a high-intensity and prolonged conflict.

- *Critical national infrastructure is vulnerable to cyber-attacks.*³ Many critical sectors of American society and business are heavily reliant on digital systems and Internet connectivity that are not sufficiently secure; 2021 witnessed 649 reported incidents of ransomware attacks on entities within critical infrastructure sectors.⁴ This ever-expanding area of attack and its indispensable role make critical infrastructure an attractive target for offensive cyber-attacks. A large-scale attack would present serious challenges for our socio-economic functioning and ability to wage war.
- *Adversaries' applications of emerging technologies may not be ethically constrained.* U.S. military operations will continue to be guided by U.S. and international law as well as the U.S. military's regulations and ethical guidelines. However, America's adversaries may not necessarily be guided by the same principles — as we see with the appalling actions of the Russian military in Ukraine. While China has not yet engaged in external military operations that have included emerging technologies in war, in a domestic law enforcement context their approach to data collection and the targeting of civilian populations in Xinjiang province raises fundamental concerns.⁵ China, in contrast to the U.S. military, has also not disclosed the existence or content of any regulations or policy directives that indicate how it intends to use emerging technologies in military operations in an ethically-responsible way. While

3 Critical infrastructure refers to those sectors that are considered so vital to the United States that their incapacitation, virtual or physical, would have a debilitating effect on national security, economic security, national public health or safety. See [Critical Infrastructures Protection Act of 2001](#), 42 U.S.C. §5195c (2001).

4 [2021 Internet Crime Report](#), Federal Bureau of Investigation at 15 (2021).

5 [Break Their Lineage, Break Their Roots](#), Human Rights Watch (2021).

the U.S. military should continue to follow law of war principles for its application of emerging technologies, it should not assume its adversaries will do the same - and it should be mindful of the advantages and disadvantages these differences create.

- *The individualization of war.* The proliferation of sensors, which collect the data exhaust that individuals leave on the Internet through everyday search, reading, watching, shopping, and dating habits, and the speed with which AI-enabled systems can analyze vast amounts of harvested data can position militaries to be able to micro-target individuals. This microtargeting is likely to entail, first and foremost, denigration campaigns and psychological pressure, but under certain circumstances could also entail targeting of key individuals with kinetic attacks. As we have seen in the Ukraine war, the Ukrainians have effectively and repeatedly tracked and targeted Russian military leaders.⁶ The effects can be delivered on the battlefield, close to it, or away from it. Individualization's greatest threat is to peacetime and crisis decision-making, but it may also contribute to disrupting large-scale combat operations.

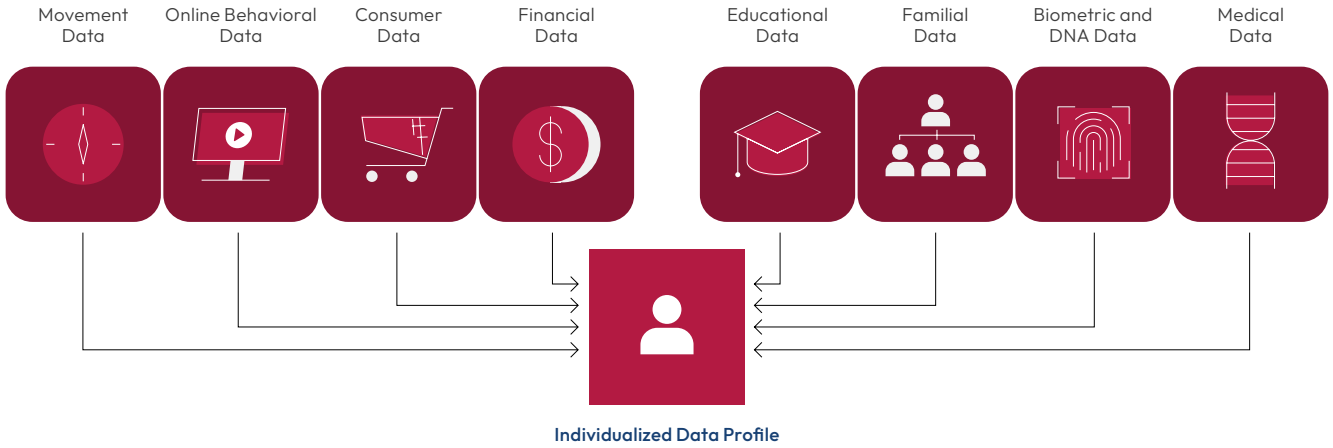
This individualization of war will change the psychology of war. On one hand, it creates the possibility of war with fewer casualties. On the other hand, the reach of new tech-enabled systems means that individual combatants, leaders, and even their family members are more easily targetable. When this takes place, anyone considered a target by the adversary will not be safe. U.S. service members, commanders, and policymakers will find themselves operating under persistent, individualized threats.

Individualization of war will also come about through further empowerment of individuals and small units who will have at their disposal increasingly more sophisticated technologies to deliver tactical to strategic effects. Individual service members are increasingly in control of a suite of strike or cyber platforms, both organic to the unit or that can be called upon to conduct an attack. As synthetic biology advances, more people can create pathogens, either from synthetic or naturally occurring DNA.⁷ By expanding the power of individuals, technology will increase uncertainty about which actions are taken by a state, by those acting on behalf of a state, or those acting on their own.

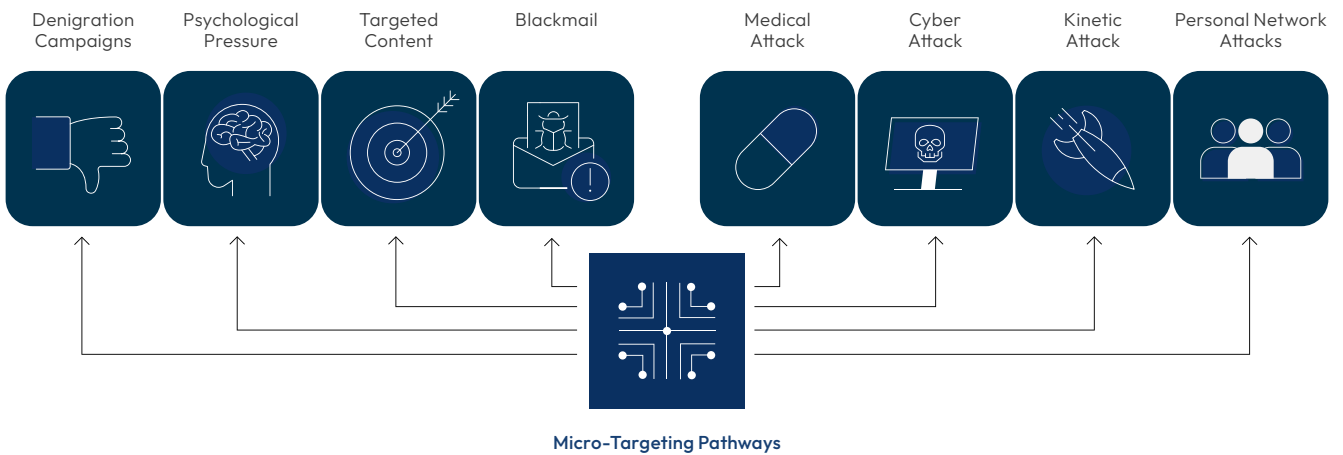
6 Julian E. Barnes, et al., [U.S. Intelligence Is Helping Ukraine Kill Russian Generals, Officials Says](#), New York Times (2022).

7 Benjamin Wittes & Gabriella Blum, [The Future of Violence: Robots and Germs, Hackers and Drones](#), Basic Books at 311-352 (2015).

Elements of Building an Individualized Data Profile



Elements of Building a Micro-Targeting Campaign



The Effects of Micro-Targeting



At the more *operational* level, we see the following dynamics:

- *Emerging technology is qualitatively changing the way we perceive our environment, communicate, and make decisions.* Mass data production and collection, behavioral tracking, and commercial imagery are increasing the availability of data for analysis, giving policymakers and military leaders much greater awareness. The application of AI and human-machine collaboration to this data will accelerate, diffuse, and compress decision-making to such an extent that at times it will seem almost instantaneous. AI can identify novel patterns and generate original insights. While cyber espionage can expose plans and intentions, increasing transparency, cyber operations can also deceive and defeat many sensors.
- *The growing importance of software and connectivity will accelerate the adaptation of tactics and military technology.* Lessons learned and software-based upgrades can be incorporated as quickly as programmers develop, transmit, and download new software. This allows software-based adaptation to bypass many of the physical and behavioral constraints of traditional adaptation. Over time, the combination of human insights and self-learning machines will allow extremely rapid changes to tactics and operating concepts.
- *The proliferation of collection platforms,⁸ analytical tools, and precision-guided munitions⁹ are fundamentally altering the hider-finder contest.* As these capabilities continue to develop and proliferate, it will become increasingly difficult to hide in every domain, including space and undersea that have traditionally been the most opaque. If adversaries more easily detect and rapidly destroy opposing forces while they are on the move, it will be difficult to employ operational surprise or tactics that rely on large formations consolidating or maneuvering, generally a key component of decisive victories. This trend will also drive a temptation for preemption, out of a desire to blind or immobilize the enemy. Restoring operational maneuver requires either subverting or overcoming enemy sensors, finding ways to restore the ability to surprise, or employing low-cost, attritable systems as part of an initial phase of operations to pave the way for subsequent attacks by regular formations.
- *Relatively inexpensive drones and loitering munitions are already changing how militaries conceive of combined arms warfare.* Drones played a prominent role in the 2020 Nagorno-Karabakh War by providing Azerbaijani forces with an aerial

8 Nishawn S. Smagh, [Intelligence, Surveillance and Reconnaissance Design for Great Power Competition](#), Congressional Research Service at 5, 7 (2020).

9 John R. Hoehn, [Precision-Guided Munitions: Background and Issues for Congress](#), Congressional Research Service at 6-25 (2021).

advantage against Armenian armor.¹⁰ Early reporting indicates drones played a similar role during the first phase of war in Ukraine,¹¹ and loitering munitions have helped Ukrainian forces destroy light and armored targets cheaply from afar.¹² Both conflicts have challenged the role that armor has traditionally played on the battlefield. As drone use in combat continues to advance and as autonomy improves, these systems will continue to change combat operations.

The People’s Liberation Army’s Theory of Victory to Defeat the U.S. Military

Over the last several decades, the United States has relied on its superior intelligence collection platforms, battle networks, and precision-guided and stand-off munitions to defeat adversaries. As adversaries develop similar capabilities, the ability of faster, more effective kill chains to realize military victory has diminished. Instead, warfare between great powers will increasingly see the confrontation of systems of sensors, networks, effects, and logistics.

For over two decades now, the PLA has closely studied the “American way of war” of guided munitions-battle networks warfare which they refer to as informatized warfare, and has worked relentlessly to adopt it for its own purposes. But the PLA has not only sought parity with the U.S. military in this regard. It has also developed a theory of victory centered around the idea of systems confrontation, whereby it would seek to destroy battle networks of its adversaries — which the PLA refers to as operational systems. This system destruction warfare aims to disrupt the flow of internal information, the time sequencing of control-attack-evaluation systems, and essential components of an adversary’s operational system through kinetic and non-kinetic means. PLA planners believe that immobilizing critical junctions in an opponent’s operational systems will isolate subsystems from critical resources and decrease overall system effectiveness.¹³ In short, they believe that military-technological parity in precision guided munitions-battle networks, and the application of their operating concept of system destruction warfare can lead them to military victory.¹⁴

10 Shaan Shaikh & Wes Rumbaugh, [The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense](#), Center for Strategic and International Studies (2020).

11 Jack Detsch, [Drones Have Come of Age in the Russia-Ukraine War](#), Foreign Policy (2022).

12 David Hambling, [Failure or Savior? Busting Myths About Switchblade Loitering Munitions in Ukraine](#), Forbes (2022).

13 Jeffery Engstrom, [System Confrontation and System Destruction Warfare: How the Chinese People’s Liberation Army Seeks to Wage Modern Warfare](#), RAND Corporation at 15-17 (2018). System destruction warfare includes but is not limited to the destruction of bases and carriers used for power projection — a move that was earlier associated with anti-access and area-denial thinking.

14 Ryan Fedasiuk, et al., [Harnessed Lightning: How the Chinese Military is Adopting Artificial Intelligence](#), Center for Security and Emerging Technology at 38 (2021).

In pursuit of a theory of victory for a potential confrontation today, the PLA has also sought to chart a path to leapfrog the United States for a potential confrontation of tomorrow. The PLA intends to capitalize on the growing capabilities of AI, big data, advanced computing, 5G, and supporting technologies to shift from informatized warfare to intelligentized warfare. By becoming the first movers in a new way of war, they hope to leapfrog the United States and become the world's dominant military power. Intelligentization includes seven trends: (1) from the strong beating the weak to the intelligent beating the dull, (2) from destructive power to manipulating cognition, (3) from human-based to human-machine collaboration, (4) from big eats small to fast eats slow, (5) from winning through integration to winning through clusters, (6) from military dominance to hybrid warfare, and (7) from practical test to experimental exercise.¹⁵

The PLA's weapon platforms and capabilities are also of increasing concern. The PLA has amassed a formidable, ever-expanding, arsenal of medium- and long-range precision missiles, including hypersonic missiles, capable of striking U.S. land and sea bases throughout the region and delaying or even preventing the United States from rapidly intervening in a crisis.¹⁶ The PLA has built a dense web of integrated air defense systems to challenge U.S. forces attempting to enter the theater of operations.¹⁷ The PRC also created the Strategic Support Force to merge information operations, including cyber, psychological operations, electronic warfare, and some space operations in an effort to operationalize system destruction warfare.¹⁸ In total, the PLA has focused on pursuing capabilities across all domains that challenge the U.S. military's ability to project power into the Indo-Pacific region, or once there, to enjoy freedom of movement and action.

United States' Asymmetric Strengths that Offer Opportunities for Advantages

While the magnitude of today's challenges may be new, this is not the first time U.S. military primacy or its ability to project power has been called into question. Moreover, the U.S. military still enjoys considerable operational and military-technological asymmetries that can be leveraged against China, to include:

- *Demonstrated Experience in Joint, Combined Arms, Expeditionary, and Networked Operations.* Combined arms operations are highly complex and demanding. Twenty years of combat in Afghanistan and Iraq, along with demanding rotations

¹⁵ Xie Kai, et al., *A Perspective on the Evolution of the Winning Mechanism of Intelligent Warfare*, China Military Network - PLA Daily (2022).

¹⁶ Christopher Mihal, *Understanding the People's Liberation Army Rocket Force: Strategy, Armament, and Disposition*, Military Review (2021).

¹⁷ Derek Solen, *PLA Army Air Defense Units Improve Effectiveness, Resiliency, and Jointness*, China Aerospace Studies Institute (2021).

¹⁸ John Costello & Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, National Defense University (2018).

at Combat Training Centers, Fleet Training Exercises, and Red Flag exercises have rendered these inherently complex operations familiar to the U.S. military.¹⁹ The PLA lacks the experience, trust, and cross-domain communication needed to effectively conduct joint and combined operations.²⁰ It has, however, recognized these shortcomings and placed a high priority on making improvements.²¹

- *Empowering Warfighters at the Lowest Tactical Levels.* The inevitable chaos of modern warfare places a high premium on the ability to adapt rapidly to meet commander's intent in the absence of regular guidance from higher headquarters.²² The U.S. military empowers its forces at the lowest level to take advantage of operational initiative and develop new solutions to fast-changing battlefield dynamics.²³ The rigid structures of the PLA, and the conformist nature of its communist political system and society, typically do not promote or reward tactical initiative and rapid adaptation.²⁴
- *Expeditionary Logistics.* The U.S. military-civilian logistics system has been one of America's greatest military strengths, both in its reach and in its ability to sustain continuous operations. This stands in stark contrast, for example, with the Russian military, which has struggled to provide logistical support for its forces in Ukraine.²⁵

However, since World War II, trans-continental and trans-regional logistics operations by the U.S. military have taken place in uncontested settings, often relying on commercial contractors to move assets and forces in a lengthy and unchallenged buildup process. By contrast, a conflict with China would likely see the PLA attack critical digital systems and physical operations in U.S. and foreign ports of embarkation and disembarkation and the logistics enterprise writ large. Such attacks could thwart the United States' ability to maintain the flow of supplies to a complex conflict abroad, particularly if the U.S. military has not prepositioned sufficient materiel and forces in advance of a crisis. In short, the U.S. military has an impressive track record of conducting expeditionary logistics, but significant

19 See e.g., Terri Moon Cronk, [U.S. Forces Work With Partners in Numerous Military Exercises](#), U.S. Department of Defense (2017).

20 Testimony of Mark R. Cozad before the U.S.–China Economic and Security Review Commission, [PLA Joint Training and Implications for Future Expeditionary Capabilities](#), RAND Corporation (2016).

21 [Military and Security Developments Involving the People's Republic of China, Annual Report to Congress](#), U.S. Department of Defense at 158 (2021).

22 [Joint Operating Environment: The Joint Force in a Contested and Disordered World](#), U.S. Department of Defense Joint Staff (2016).

23 [Mission Command: Insights and Best Practices Focus Paper](#), U.S. Department of Defense Joint Staff, Deployable Training Division at 3 (2020).

24 Mark Cozad, [Toward a More Joint, Combat-Ready PLA](#), National Defense University Press (2019).

25 Jim Garamone, [Ukrainian Resistance, Logistics Nightmares Plague Russian Invaders](#), U.S. Department of Defense (2022).

preparations need to be undertaken to retain this important advantage in the contested environment of an Indo-Pacific fight, where the vast distances involved, attacks on infrastructure, and the limited logistical throughput of the region can cripple operations. The PLA for its part has made efforts to strengthen its own untested expeditionary logistical capabilities.²⁶

- *Allies, Partners, and Global Posture.* The United States has far more and much deeper alliances and partnerships than China, which has few or no allies. This advantage would enable the United States to generate greater diplomatic legitimacy, build military mass, create broader and deeper multi-domain effects, attack from different axes, and coordinate intelligence across a much larger network. The U.S. military's expeditionary capabilities and consistent forward presence in key regions, particularly astride critical global choke points, further strengthen the U.S. global posture.²⁷ This also makes it easier for the United States to rapidly deploy capabilities, employ military assets and forces, and sustain expeditionary logistics. At the same time, the United States military must be prepared for the possibility that not all allies or partners would join in a potential conflict with China, or even allow U.S. military forces to operate from their territories. Developing a more precise understanding of which nations may or may not grant U.S. access during wartime, and identifying those which are essential to U.S. military operations would mitigate some of the operational risks.
- *The Strengths of a Democratic Society.* Individual freedoms and empowerment — characteristic of democratic societies — foster innovation, entrepreneurship, and initiative. This makes the United States more resilient, agile, and more likely to adapt successfully to changing conditions. This empowerment of the individual and encouragement of initiative is also reflected in the U.S. military services. Additionally, the United States has deliberately pursued and built a professional and apolitical military force, which stands in stark contrast to the PLA. The PLA has a long history of corruption and coup-proofing.²⁸ Both tendencies lead to promotions based on political loyalty rather than competency, a lack of trust in junior leaders, a lack of tactical initiative, an aversion to speaking truth to power, and ineffective decision-making due to less candid discussion during the planning process.²⁹ They

26 Chad Peltier, [China's Logistics Capabilities for Expeditionary Operations](#), Jane's at 4 (2020).

27 Michael Tanchum, [China's New Military Base in Africa: What it Means for Europe and America](#), European Council on Foreign Relations (2021); Hal Brands, [America and China Are in a Global Fight Over Military Bases](#), Bloomberg (2021); [Where Are U.S. And Russian Military Bases In The World](#), RadioFreeEurope, (2015).

28 Dennis J. Blasko, [Corruption in China's Military: One of Many Problems](#), War on the Rocks (2015).

29 Thomas Carothers & David Wong, [Authoritarian Weaknesses and the Pandemic](#), Carnegie Endowment for International Peace,

also contribute to the wasting of resources, and uncertainty in performance during conflict. These political constraints lead militaries to struggle to perform in chaotic conditions and during communication breakdowns, or to make significant, on-the-fly adjustments during combat missions. Phrased differently, in this system, regime security overrides national security.³⁰ Authoritarian state stability relies on near total control, not resilience. Finally, China's long-time pursuit of the one-child policy weakens its military strength.³¹ While the PLA will necessarily suffer a shortage of military personnel, any contingency that results in casualties will cause many families to lose their only child, resulting in considerable political blowback.

From Asymmetries to Advantages: An Offset-X Strategy

As we look towards 2025-2030, a war between great powers is more likely than it has been in generations. Emerging technologies are impacting the way militaries understand their environment and make decisions. Some of these same technologies will continue to change the tools of war, operational concepts, and how violence can be employed for political outcomes. While combat in traditional domains could still play a significant role, warfare will also be waged with and against industrial and financial power and pit innovation ecosystems against each other. It will be conducted across continents and borders and target individuals in new ways. It will be determined by political will as much as any other factor.

Over the last several decades, the United States has relied heavily on its superior intelligence collection assets, stand-off platforms, precision-guided munitions, highly-trained personnel, and expeditionary logistics to defeat adversaries. But advanced and emerging technologies are changing the reliability and effectiveness of these systems. Moreover, adversaries have developed some of the same capabilities, invested heavily in neutralizing America's operational superiority, and focused on diminishing the ability of the U.S. military to employ faster, more effective kill chains. In this changing technological-military landscape, the PLA aims to, in a crisis or war, paralyze the U.S. body politic, bring America's economy to a standstill, immobilize the U.S. military by destroying its battle networks, and present U.S. leaders with serious doubts about their ability to support partners and allies, leaving them with almost with no other option but to concede. Amid the uncertain overmatch for traditional U.S. military capabilities, the outcome of a potential

(2020).

30 Caitlin Talmadge, [The Dictator's Army: Battlefield Effectiveness in Authoritarian Regimes](#), Cornell University Press (2015).

31 Feng Wang, et al., [The End of China's One-Child Policy](#), Brookings (2016); see also [One-Child Policy 'Weakens China's Military'](#), Radio Free Asia (2012); [China Grappling with Effects of 'One-Child Army'. Adds Unmanned Aircraft, Ballistic Missiles, Says Experts](#), Yahoo News (2021).

war by the end of the decade with the PLA will increasingly come down to the superiority and resilience of sensors, networks, software, interfaces between humans and machines, logistics, and – especially – the systems that tie or empower them all together. It will also come down to the U.S. willingness and ability to insert itself now within the PLA’s envisioned future battlespace.³²

In response to these challenges, we outline a new approach – an Offset-X strategy – that could lay the groundwork for the United States to restore its military-technological superiority, and in the process circumvent China’s military advancements, thwart its theories of victory, restore America’s ability to project power in the Indo-Pacific region, and position the United States to honor its commitments to the stability of the region. This approach is derived from and grounded in America’s persistent, asymmetric strengths, and envisions the deployment and employment of new capabilities in ways that China will struggle to match or quickly duplicate. It aims to minimize the human and political cost the United States and its allies would suffer during a war with China, while driving up the political costs of war and creating serious dilemmas for Chinese leadership.

The initiatives we outline below are, by no means, a comprehensive or definitive list of actions. Together, they embody a competitive strategy to achieve and maintain military-technical superiority over all potential adversaries. However, no offset strategy against China should be treated as set in stone. Rather, it needs to be regularly reassessed against the PLA’s adaptations, and should continuously seek to leverage emerging technologies. But we believe that the following initiatives provide a good starting point:

This approach is derived from and grounded in America’s persistent, asymmetric strengths, and envisions the deployment and employment of new capabilities in ways that **China will struggle to match or quickly duplicate**. It aims to minimize the human and political cost the United States and its allies would suffer during a war with China, while driving up the political costs of war and creating serious dilemmas for Chinese leadership.

³² The United States Marine Corps Force Design 2030, intended to help prevent the People’s Liberation Army Navy from pushing past the First Island Chain, is a first effort to confront the PLA’s systems, rather than just close kill chains. SCSP Defense Panel Meeting (July 2022). For additional details, see [Force Design 2030](#), U.S. Marine Corps (last accessed 2022).

Offset-X Strategy

A competitive strategy to achieve and maintain military-technological superiority over all potential adversaries.



Recommendations

- ▶ Fully Embrace Distributed, Network-based Operations.
- ▶ Lead the World's Militaries in Human-Machine Collaboration and Human-Machine Teaming.
- ▶ Gain and Maintain Software Advantage.
- ▶ Ensure Resilience in Our Ability to Sense, Communicate, Attack, and Supply.
- ▶ Undermine Adversary's Censorship System.
- ▶ Undermine Adversary's C3 Systems.
- ▶ Evolve Deliberate War Planning.
- ▶ Help Allies and Partners Develop Interchangeability with U.S. Forces.
- ▶ Implement a New Public-Private Partnering Model with Industry, Academia, Investors, and Civil Society.
- ▶ Develop and field counter-autonomy.

- *Fully Embrace Distributed, Network-Based Operations to Survive, Out-Maneuver, and Overwhelm Adversaries.* Confronted with adversaries that value rigid hierarchies and have invested in capabilities that could provide them with some protection against concentrated, frontal assaults, the U.S. military should continue to develop and experiment with how it will employ smaller, highly-connected, and organically resilient, multi-domain units that practice network-based decision-making and effects, not just hierarchy-based decision-making.³³ Such units would operate in a distributed fashion, inside and outside an adversary's envisioned battlespace. Such a network could generate significant dilemmas for the adversaries by creating multiple attack vectors and cross-domain effects. When acting in concert, distributed, networked forces can create mass, generate compounding effects, and operate with greater adaptability than single systems. When acting in isolation, they can distract and create new windows of operational opportunities, especially for follow-on, more conventional formations.

While the components of Offset-X strategy outlined here do not contain any recommendations on lethal autonomous weapon systems (LAWS), SCSP maintains that any application of emerging technologies for military purposes can and should be done in ways that are **consistent with the laws of armed conflict**. The U.S. Department of Defense has taken serious steps to ensure they have procedures and policies in place to responsibly field these capabilities.³⁴

- *Lead the World's Militaries in Human-Machine Collaboration and Human-Machine Teaming.* Essential to the concept of distributed, but highly-networked forces will be an extensive network of low-cost sensors, satellites, and reconnaissance platforms, as well as large numbers of attritable unmanned systems operating at sea, in the air, and on the ground to expand attack surfaces and absorb lethality. Employing them effectively, however, will require mastering human-machine cognitive collaboration (HMC) and human-machine combat teaming (HMT). HMC and HMT are assuming center stage in several states' visions for the future of warfighting, and have the potential to considerably change warfare. For the U.S. military, human-machine cognitive collaboration will be critical to optimizing decision-making. Human-machine combat teaming, meanwhile, will be essential

³³ [Force Design 2030](#), U.S. Department of the Navy at 6 (2020).

³⁴ [U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway](#), U.S. Department of Defense (2022); Kathleen Hicks, Deputy Secretary, [Memorandum for Senior Pentagon Leaders on Implementing Responsible Artificial Intelligence in the Department of Defense](#), U.S. Department of Defense (2021); DoD Directive 3000.09, [Autonomy in Weapon Systems](#), U.S. Department of Defense (2012).

for more effective execution of complex tasks, especially higher-risk missions, or in confronting an adversary with sophisticated autonomous systems.

A core concept of HMC and HMT is that humans and machines have comparative advantages and therefore excel in different areas.³⁵ Humans outperform machines on many sensory tasks, certain types of communication, high-context tasks requiring intuition, and various types of creative exploration. Machines often outperform humans at tasks that require processing extremely large volumes of data, a high degree of precision, memory, and consistent repetition. Augmenting human limitations with machine strengths (and vice versa), can create human-machine collaboration and teaming that outperform both humans and machines in many of their individual tasks. This may involve faster AI-powered decision-making, rapid processing and analysis of intelligence, surveillance, and reconnaissance (ISR) data, and combat tasking with autonomous systems, such as AI co-pilots.³⁶ Also, machines are vastly better suited for high risk-to-force missions.

HMC focuses primarily on cognitive tasks. A warfighter's mental bandwidth, as for every human, is limited. A decision to spend time solving one problem is a decision not to spend time on an equally critical task. The growth of HMC will enable individuals to break problems into their component pieces³⁷ and task some to be optimized, automated, or performed at scale by a computer in order to remove some of the clutter that taxes so much cognitive energy and free that up for higher order processing. It will also allow individuals to refocus their mental bandwidth towards gaining situational awareness, understanding enemy plans, developing courses of action, accomplishing far more than they would otherwise, and mastering the tasks that humans do best.

Meanwhile, human-machine combat teaming could enable the U.S. military to generate and employ mass in contested environments and do so in a way that reduces the risk to humans,³⁸ including risks of collateral damage. By employing lower-cost, easier-to-manufacture, and AI-enabled machines, new frameworks can be developed that leverage autonomy to permit operators and machines to overcome challenges of complexity so that what was once a single thing becomes a team of things. Single, expensive platforms cannot achieve the same diversity of use

35 Tony Ojeda, [The Algorithm - Human Tasks vs Machine Tasks](#), District Data Labs (last accessed 2022).

36 Julie Obenauer Motley, [The Testing and Explainability Challenge Facing Human-Machine Teaming](#), Brookings Tech Stream (2022).

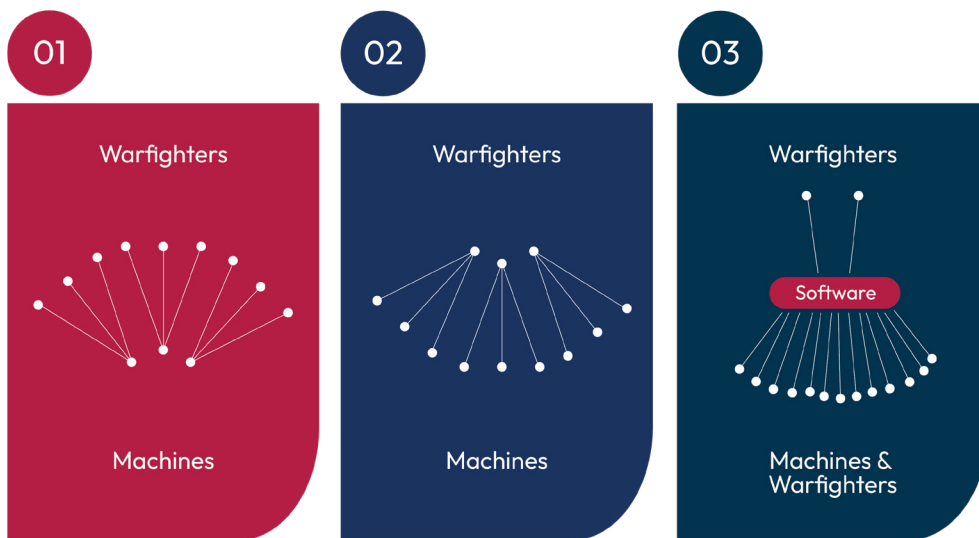
37 [What Is Computational Thinking?](#), Center for Computational Thinking, Carnegie Mellon University (last accessed 2022).

38 John Laird, et al., [Future Directions in Human Machine Teaming Workshop](#), U.S. Department of Defense at 3 (2019).

as swarms of inexpensive systems. Massed machines, assigned tasks by their human teammates, could overwhelm traditional defenses, often at a relatively smaller cost in human casualties compared to more traditional offensive operations. Machines could also serve as the “eyes and ears” of their human teammates, particularly in urban warfare, by helping them gain more information about their environment and taking risks in their place.

Another change that HMT can bring is in the balance of mass and effects delivery away from humans and towards machines. Today, in most cases, many warfighters collectively control one platform, such as a ship. While that relationship is unlikely to vanish, another human-machine relationship is developing that could begin to chip away at the dominant warfighter-platform relationship. One such mode is AI-powered architectures that leverage the contextual awareness and complex reasoning of human operators to manage large numbers of autonomous and semi-autonomous unmanned systems, as well as warfighters. An example of the potential of such an approach can be seen in DARPA’s OFFensive Swarm-Enabled Tactics (OFFSET) program.³⁹

Human-Machine Collaboration and Teaming



HMC and HMT are not mutually exclusive concepts. Many applications, especially more advanced applications, will include elements of both. Also, while HMC and HMT are not analogous to autonomy, they will rely on autonomy for their

³⁹ [OFFSET Swarms Take Flight in Final Field Experiment](#), Defense Advanced Research Projects Agency (2021).

effectiveness, especially during high-intensity conflicts. Autonomous systems can perform tasks assigned to them by human operators to increase or amplify U.S. military presence, persistence, and effectiveness, while reducing the risks and costs of operations, particularly in urban environments. HMC and HMT, thus, can serve as an engine of greater autonomy, where appropriate, by helping develop and test capabilities, human-machine interfaces, and the military's ability to employ semi-autonomous or autonomous systems effectively and responsibly.

By 2030, the U.S. military should fully integrate HMC and HMT into daily operations at the tactical, operational, and strategic levels. The military services should prioritize development, accelerate adoption, and integrate training on HMT in military schools and training centers. Combatant Commands should identify opportunities and take actions to integrate HMC and HMT into their operations at all levels, irrespective of progress at the level of services or Department. The near-term priority should be to develop the most sophisticated interfaces for HMC and HMT while exploring the degree of autonomy assigned to unmanned systems, consistent with U.S. Department of Defense policy and international law.

- *Gain and Maintain Software Advantage.* A military's ability to deploy, employ, and update software, including AI models, faster than its adversaries is likely to become one of the greatest determining factors in relative military strength. Software is now integral to every component of decision and kill chains, from sensing a target (sensor software) to decision-making (aggregation and analysis), targeting (weapons guidance system), and battle damage assessment.⁴⁰ The importance of software will only continue to increase. As militaries around the world increasingly rely on platforms with advanced computing capacities, and supplement or even replace some functions of human service members with algorithms, software superiority will become an even greater determining factor.⁴¹ The quality of software will determine a military's ability to collect and analyze information, develop an operating picture, thwart enemy attacks, identify opportunities in time and space to most effectively attack, and help with target selection and servicing.

Software already shapes how militaries organize, coordinate, and employ all of the elements of national power. Software can also facilitate a shift from a small number of very exquisite satellites to a large number of significantly less expensive and less capable systems, but whose integration through software can produce the

40 [Department of Defense Software Modernization Strategy](#), U.S. Department of Defense at 1-2 (2022).

41 [Software Acquisition and Practices \(SWAP\) Main Report](#), U.S. Department of Defense, Defense Innovation Board (2019).

same information as the existing, expensive satellites. Such a constellation of low-cost, space-based assets could also play a critical role in defending against missile attacks, particularly hypersonic missiles that challenge existing paradigms of in-flight tracking.

Similarly, the DoD also needs to adopt a new information architecture that will allow the DoD to be far more flexible, scale on demand, and adapt dynamically to changing conditions. As recommended by the National Security Commission on AI, this would include access to cloud computing and storage;⁴² a secure, federated system of data repositories with appropriate access controls; a secure network with the bandwidth needed to support data transport; common interfaces; development environments; and shared development resources that allow commands to quickly access the data, software, and models they need. The military also needs new specialties for tactical software development and management.⁴³ At the operational and tactical levels, in order to more fully capture the power of software and accelerate its development, the U.S. military should empower its tactical units to experiment with, develop, and deploy robust, reliable, and resilient software for the capabilities that they operate. In short, the U.S. military should aim to develop every future system and capability with a software-centric orientation in mind.

- *Ensure Resilience in Our Ability to Sense, Communicate, Attack, and Supply.* In a conflict with China, system destruction warfare would indicate that one of the PLA's opening moves will be directed at U.S. forces' ability to see them, listen to them, and locate them precisely. Simultaneous or follow-on attacks will likely target the ability of U.S. military leaders to command and control their forces. Additional attacks will almost certainly be aimed at the U.S. military's ability to logistically sustain its operations. Blind, deaf, and unable to communicate, U.S. forces will be paralyzed.

To avoid this paralysis, the U.S. military needs to build resilience, and where necessary, redundancies across every link and node of its operations — from sensors to attack platforms, in information architecture and networks, across command and control, for logistics, and for humans. This includes both terrestrial and space-based systems and networks. Resilience can come from acquiring and using very large numbers of low-cost and attritable platforms that would support intelligence

42 [Department of Defense Software Modernization Strategy](#), U.S. Department of Defense at ii (2022).

43 [Final Report](#), National Security Commission on Artificial Intelligence at 59-69 (2021); [U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway](#), U.S. Department of Defense (2022); Kathleen Hicks, [Memorandum for Senior Pentagon Leaders on Implementing Responsible Artificial Intelligence in the Department of Defense](#), U.S. Department of Defense (2021); DoD Directive 3000.09, [Autonomy in Weapon Systems](#), U.S. Department of Defense (2012).

collection, communication, logistics, and attack — especially during the opening days of a campaign. And operational resilience will also require strategic resilience, which will be heavily dependent upon our ability to harden now the nation’s critical infrastructure from cyber-attacks.

- *Undermine Adversary’s Censorship System.* Authoritarian regimes are brittle, relying more on information control than buy-in to maintain domestic stability. As such, they are vulnerable to operations that allow their populations to more easily and consistently bypass censorship systems and access information other than state propaganda. In the context of war, such operations — including AI-enabled messaging to circumvent censorship — have the potential to distract authoritarian regimes by increasing their focus on domestic security, to the detriment of their offensive operations. This would be especially important during a Chinese attempt to capture Taiwan by force. By helping ordinary Chinese citizens during times of war thwart automatic censors and by placing the burden on regime human censors, the United States can help expand the public discourse beyond the regime’s control.
- *Undermine Adversary Command Systems.* The United States should also consider how it can subvert the effectiveness of adversary command, control, and communication (C3) systems. If the United States were to disrupt or cripple the PLA’s C3 systems, it would cause disarray among the ranks of the PLA and desync its operations, preventing it from massing effects against U.S. forces. Preparing such offensively oriented operations, however, should be accompanied by defensive preparations. The U.S. military needs to be prepared, preferably with AI-enabled capabilities, to detect and defend against operations that flood our society with misinformation or undermine U.S. command, control, and communications systems.
- *Evolve Deliberate War Planning.* Traditionally, DoD’s deliberate war planning is based on the existing inventory of capabilities and forces. Planning guidance documents have generally instructed Combatant Commanders to construct war plans, and associated time-phased force deployments data (TPFDD), based on the capabilities available to them, in the first instance, and additional capabilities that could be allocated to them in the event of conflict from the total inventory.⁴⁴

This approach to deliberate war planning, however, may no longer be suited for the anticipated changes in the character of warfare during this decade. First, the current method of planning does not factor in the state of the defense industrial base and its ability, or lack thereof, to surge production of munitions or

44 DoD Instruction 3000.15, [Plan Review and Approval Process](#), U.S. Department of Defense at 11 (2020).

platforms.⁴⁵ This could result in serious strategic risks, particularly in the event of high-intensity operations that rapidly consume existing inventory of munitions and assets, or in the event of a protracted conflict. In other words, the current method of war planning runs the risk of producing a situation in which the U.S. military could run out of munitions or assets before reaching the end of conflict. Second, the resource straight-jacketing embedded in the current planning methods limits the development of innovative concepts and reduces the ability of Combatant Commanders to influence the development of new capabilities.

Put another way, Combatant Commanders are not encouraged to identify new disruptive technologies and develop corresponding concepts of operations that could lower the risk to force and mission. Therefore, the Defense Department should seriously consider evolving its deliberate war planning guidance documents and methodology, by considering the health and resilience of the defense industrial base and the full potential of the national security innovation network. This updated approach will likely result in plans that combine rigorous risk assessments with more effective operational solutions. This could also help DoD identify and prioritize the development and fielding of new, innovative capabilities.

- *Help Allies and Partners Develop and Maintain Interoperability and Interchangeability With U.S. Forces.* As the United States continues to modernize its military forces, including investments in emerging technologies, there is a risk that a gap in capabilities between the United States and its allies could become a serious impediment to combined operations. Some of this gap is due to under-investments in defense by allies. Some of it has to do with security practices, particularly regarding the transfer of technologies, intelligence sharing, and command and control (C2) operations. But an important part of this gap also comes from the fact the United States has access to a unique innovation ecosystem. The United States must address these challenges if it is to capitalize on one of its most enduring asymmetries against China — the network of alliances and partnerships. In the near term, a promising action could be the establishment of a multilateral intelligence, surveillance, and reconnaissance network to improve coalition awareness in peacetime, and enable a more rapid transition from crisis to conflict during wartime.⁴⁶ Another action could be the development of a Joint and Combined All Domain Command and Control

⁴⁵ For more details on the challenges related to the U.S. techno-industrial base and near-term recommendations, see Chapter 2 of this report.

⁴⁶ Becca Wasser, Developing Integrated ISR Networks to Improve Coalition Responsiveness, Presented at SCSP Defense Panel Meeting (July 2022).

(JCADC2) architecture. This would be the multilateral expansion of the current U.S.-only Joint All-Domain Command and Control (JADC2) concept.⁴⁷ But the U.S. Government must accept far greater risks in information sharing and transfer of technologies to make this successful.

- *Implement a New Public-Private Partnering Model Between the U.S. Government, Industry, Academia, Investors, and Civil Society.* One of America's greatest defense strengths in the past has been the close collaboration between the government, industry, and academia. That collaboration has, for various reasons, suffered over the past twenty years. At the same time, the CCP has been focusing on comprehensive national military-civil fusion.⁴⁸ China continues its inexorable march toward reducing dependencies on the United States and advancing the development of Chinese technology companies. The United States must make a concerted effort to restore the level of collaboration between the government, industry, and academia, and to accelerate the adoption of commercial technology by the DoD. The defense industry played an essential role in developing capabilities that enabled the United States to prevail in the Cold War and conduct stability and counterterrorism operations in its aftermath and is already playing a critical role in the current geopolitical and technological contest. Just as importantly, collaboration must also extend to private investors and civil society. Civil society plays an important role in helping decide how technology should be employed, both for national security and civilian purposes. Private investors can bring to bear far greater capital towards the development and deployment of technology than the federal government. If the United States is able to unite all five stakeholders to pursue specific goals, America's dynamic market capitalist system and innovative commercial sector is much more likely to prevail over the long term. If not, the United States risks ceding critical ground to China.
- *Develop Counter-Autonomy.* As the U.S. military integrates more AI, human-machine teaming, and autonomy, adversaries can be expected to do the same. The U.S. military should, therefore, develop capabilities and concepts for countering adversary autonomy. In the near term, the focus of U.S. counter-autonomy efforts could include identifying means and generating access to take over adversaries' AI-enabled systems to extend our sensing deep inside their territory and within its decision-making. During conflict, counter-autonomy efforts could include actions to manipulate the data or outputs of adversarial AI-enabled systems so as to inject

⁴⁷ [Summary of the Joint All-Domain Command & Control \(JADC2\)](#), U.S. Department of Defense (2022).

⁴⁸ [Military-Civil Fusion and the People's Republic of China](#), U.S. Department of State (2020).

mistrust between their forces and their machines, degrading the performance of their AI-enabled and autonomous systems, or destroying them entirely through kinetic or non-kinetic means.⁴⁹ While the immediate focus of the U.S. military should remain on developing its own autonomous systems, the United States cannot afford to wait for too long to develop the ability to counter and defeat adversarial AI-enabled and autonomous operations.

Operationalizing the Offset-X Strategy

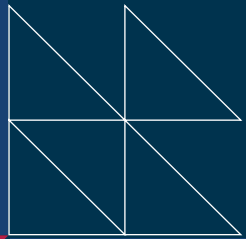
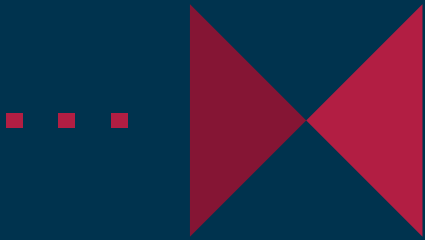
The ten recommendations outlined above embody a competitive strategy to lay the groundwork for achieving and maintaining military-technical superiority over all potential adversaries. They are not intended as nor should be viewed as an operational prescription. Significant prototyping, experimenting, and wargaming will need to be undertaken to validate the applicability and effectiveness of various innovative technologies for specific operational demands. The precise mix of emerging technologies and capabilities will yet need to be determined to address the changing character of warfare and peace. But as with previous successful offset strategies, the national and DoD pursuit and mastery of emerging technologies and innovation can enable the crafting of new operational concepts that can be tailored to meet specific military challenges. Offset-X strategy aims to build the foundation for future operations that can more easily and quickly offset adversarial capabilities.

⁴⁹ [Counter Autonomy: Executive Summary](#), U.S. Department of Defense, Defense Science Board at 3 (2020).

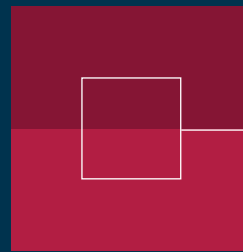
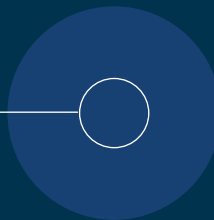
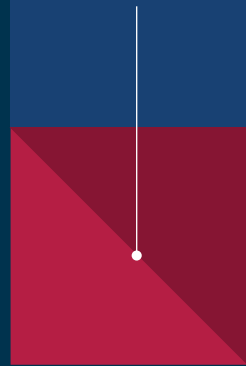
Intelligence in an Age of Data-Driven Competition

Mid-Decade Challenges to National Competitiveness

06



- Adapting U.S. Intelligence for the Digital Era
- Leveraging Open Source Capabilities
- Creating Techno-Economic Intelligence
- Countering Foreign Adversarial Influence Operations



CHAPTER 6

Intelligence in an Age of Data-Driven Competition

The mid-decade challenge for the U.S. Intelligence Community is winning the accelerating race for actionable insight to enable U.S. statecraft in a more information-rich and geopolitically competitive world.

For the first time since the Cold War, the United States faces a rival – the People’s Republic of China – that is competing globally across the economic, political, social, and military domains to lead, if not dominate, the international order. For the U.S. Intelligence Community, this rivalry will shape not only what U.S. leaders ask of it, but also how it must evolve to meet this challenge. In a rivalry with a technological and economic near-peer, providing insight into emerging technologies and the organizations that field them is as important as understanding the traditional political and military institutions of a state.¹

In addition to the geopolitical rivalry, the exponential increase in surveillance, monitoring, and collection technologies are creating avalanches of data. Like all U.S. Government organizations, the IC

In a rivalry with a technological and economic near-peer, providing insight into **emerging technologies and the organizations that field them** is as important as understanding the traditional political and military institutions of a state.

¹ Corin Stone, [A Roadmap for AI in the IC](#), The Cipher Brief (2021); Amy Zegart, [American Spy Agencies Are Struggling in the Age of Data](#), Wired (2022); Corin Stone, [Artificial Intelligence in the Intelligence Community: The Tangled Web of Budget & Acquisition](#), Just Security (2021).

faces challenges to collect, process, and analyze it. Once government-unique capabilities, like geospatial² and signals intelligence,³ have been commercialized. Private companies can now provide tailored analytic products to U.S. Government consumers on breaking events, sometimes ahead of the IC, in part because they are equipped to use AI and other emerging technologies. These companies can also select contracts or exploit opportunities that specifically showcase their strengths.⁴ Meanwhile, policymakers' demand for insight across an ever-broader array of issues may lead them to turn more frequently to the private sector and academia, or to try and find the data they need on their own in the public domain.

For its part, the IC remains predominantly human-centric, relying on methods that are manually intensive and lack scalability, despite some pockets of technological excellence. Compounding that problem, the IC is still transitioning from countering terrorism to supporting the geopolitical competition with the PRC (and Russia). However, the IC remains essential. Amidst a flood of data and opinion, the IC's emphasis on objectivity and providing insight independent of policy give it a vital role in supporting leaders grappling with difficult decisions.

IC leaders appear to understand the challenges of this new era of techno-economic competition. They were among the first in the U.S. Government to experiment with AI,⁵ with numerous AI projects,⁶ organizational shifts,⁷ and new efforts to capture data outside government channels.⁸ They recognize that once-unique U.S. collection capabilities are now known and used by foreign intelligence services. The PRC and other hostile actors exploit this knowledge and the opportunities afforded by ubiquitous technical surveillance

2 Todd Harrison & Matthew Strohmeier, [Commercial Space Remote Sensing and Its Role in National Security](#), Center for Strategic and International Studies (2022).

3 Cortney Weinbaum, et al., [SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain](#), RAND Corporation (2017).

4 Elizabeth Leyne & Yvette Nonté, [Is the Intelligence Community Staying Ahead of the Digital Curve? A Survey of its Highest-level Customers and Leaders on the Challenges and Opportunities Ahead](#), Harvard University - Belfer Center for Science and International Affairs (2021).

5 Maxime Fischer-Zernin, [Narrative Science: The CIA is Investing in Artificial Intelligence That Actually Works](#), Mic (2013).

6 [The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines](#), Office of the Director of National Intelligence (2019); [DIA's "MARS" Initiative Reaches Another Key Milestone](#), Defense Intelligence Agency Public Affairs (2021); [NGA Releases New Data Strategy to Navigate Digital, GEOINT Revolution](#), National Geospatial-Intelligence Agency (2021); Sarah Scoles, [Meet the US's Spy System of the Future — It's Sentient](#), The Verge (2019); Mark Pomerleau, [NSA's Cybersecurity Directorate Looks to Scale Up This Year](#), C4ISRNET (2022); Patrick Tucker, [What the CIA's Tech Director Wants from AI](#), Defense One (2017).

7 See e.g., [Organization: Directorate of Digital Innovation](#), U.S. Central Intelligence Agency (last accessed 2022); Quint Forgey & Daniel Lippman, [CIA Launches New China-Focused Unit](#), Politico (2021).

8 Steven Aftergood, [Open Source Center \(OSC\) becomes Open Source Enterprise \(OSE\)](#), Federation of American Scientists (2015); Justin Doubleday, [Spy Agencies Look to Standardize Use of Open Source Intelligence](#), Federal News Network (2022); Justin Doubleday, [State Department Intelligence Arm to Set Up Open Source Coordination Office](#), Federal News Network (2022).

...the IC's ability to **provide competitive advantage** to U.S. policymakers will hinge on whether it can master emerging technologies, including AI, to integrate more and more diverse information across all domains.

to become global counterintelligence threats.⁹ As the PRC builds out digital infrastructure globally, U.S. intelligence will more frequently operate where Beijing can apply its own technology-enabled tools, including AI and biotechnology, to expose its operations.¹⁰ The IC leadership's understanding and attempts to address the problem, however, have not yet translated into sustainable, community-wide change.

In this new context, the IC's ability to provide competitive advantage to U.S. policymakers will hinge on whether it can master emerging technologies,

including AI, to integrate more and more diverse information across all domains. The IC's ability to unlock new insights in support of U.S. statecraft will hinge on whether it can take action in the following areas:

- *Adapt* to the technological era and rivalry through digital transformation by integrating people, process, and technology to exploit a wider body of data in support of national security;
- *Leverage* insights and information through open source capabilities by creating a dedicated, technology-enabled open source entity to support U.S. decision making;
- *Create* new capacities to capture and master economic, financial, and technological intelligence by establishing a National Techno-Economic Intelligence Center to serve as an economic "nerve center" for U.S. policymakers; and
- *Counter* foreign adversarial influence operations by preemptively exposing them when possible, warning of them when strategically consequential, and alerting senior U.S. Government officials who may be targeted by such operations.

⁹ Zach Dorfman & Jenna McLaughlin, [The CIA's Communications Suffered a Catastrophic Compromise. It Started in Iran](#), Yahoo News (2018); Zach Dorfman, [Tech Giants Giving China an Edge in Espionage](#), Foreign Policy (2020).

¹⁰ Samantha Hoffman & Nathan Attrill, [Mapping China's Tech Giants: Supply Chains & the Global Data Collection Ecosystem](#), Australian Strategic Policy Institute (2021).

AI Use Cases for Intelligence

Tasking

- Sequencing and deconflicting the tasking of intelligence platforms efficiently across collection disciplines.
- Detecting and prioritizing targets of interest by analyzing patterns that suggest opportunities to collect unique information or exploit vulnerabilities.
- Assisting decision-makers in identifying information requirements and prioritizing collection targets.

Collection

- Identifying potential opportunities for collection by finding gaps in tech-enabled counterintelligence and security systems as well as alternative collection pathways to an intelligence target.
- Automating the validation process by cross-checking collection across all other reporting and collection disciplines.
- Enabling smart sensors at the edge to improve collection fidelity and trigger collection when necessary.

Processing

- Transforming unstructured data into a structured queryable, filterable, sortable, and digestible data to aid analysis.
- Employing natural language processing to transcribe, translate, and summarize foreign language materials.
- Summarizing raw intelligence reporting with critical information highlighted and tailored for analysts.

Analysis

- Accelerating pattern matching and anomaly detection across intelligence disciplines and the intelligence record.
- Generating visualizations to illustrate relationships, networks, geographies, and time lapses.
- Automating portfolio-specific indications and warning alerts for analysts.

Dissemination

- Tracking usage and impact of disseminated intelligence reporting and analysis.
- Automating the creation and delivery of finished and raw intelligence to the appropriate users and analysts at any level of classification.
- Streamlining classification downgrading to facilitate intelligence sharing with other U.S. Government agencies, allies, and private industry.

Business Practices

- Systematizing the auditing and approval process for routine business practices, such as accounting, as well as flagging anomalies for manual review.
- Monitoring IT systems to provide predictive maintenance and upkeep requests.
- Supporting the workflow and review requirements for Contracting Officer's Technical Representatives through a project's life cycle.

Security

- Strengthening physical security measures by enhancing network video surveillance, trace detection, and other intrusion detection systems.
- Augmenting security clearance investigation and continuous evaluation.
- Mapping supply chains of IC vendors and equipment.

This transition will not be easy. The White House and Congress must set the direction while IC leaders sustain focus within the bureaucracy for forward movement. Policymakers and members of Congress must agree to a vision on how to urgently reform the IC based on the current technology trends and geopolitical threats. The closed nature of U.S. intelligence — a requirement for keeping secrets — has often allowed inertia to persist. When united under a common goal, however, the IC is capable of remarkable transformation as it demonstrated after the September 11, 2001, terrorist attacks. The stakes of the moment demand that U.S. intelligence overcome the bureaucratic resistance to change.

Adapting U.S. Intelligence for the Digital Era

U.S. intelligence is capable of delivering on the seemingly impossible and the once-unthinkable. The IC was able to successfully warn the White House, Ukraine, and its allies of the Russian invasion long before its actual occurrence.¹¹ The early and rapid declassification of this intelligence countered Russian disinformation credibly, dissuaded the possibility of false flag operations, and undermined the Kremlin narrative.¹² This kind of performance is made possible by the IC — along with its U.S. Government partners — operating the world's largest constellations of human and machine sensors located anywhere from undersea to outer space. The IC benefits from the accumulated data even when it struggles to process it, and all while looking at the world outside the range of its sensors. U.S. intelligence faces a paradox of simultaneously having both too much and too little data.¹³

As the IC becomes increasingly involved in countering rivals and enabling U.S. and allied actions, one key to winning the techno-economic competition will be employing emerging technology tools, especially AI, to turn troves of data — and the correct type of data — into a wealth of intelligence that enables U.S. policymakers to act.

Mastering AI and emerging technologies has the potential to transform the IC. Top-down leadership is needed to drive and sustain this transformation. Success in AI and emerging technologies starts with the right leadership culture that is committed to the endeavor and willing to devote time and resources.¹⁴ Transformation requires adherence to a coherent vision that aligns strategies, actions, incentives, and metrics. IC leaders must understand

11 Shane Harris & Paul Sonne, [Russia Planning Massive Military Offensive Against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns](#), The Washington Post (2021).

12 Felicia Schwartz & Demetri Sevastopulo, [A Real Stroke of Genius: US Leads Efforts to Publicise Ukraine Intelligence](#), Financial Times (2022); [Press Briefing by Press Secretary Karine Jean-Pierre and NSC Coordinator for Strategic Communications John Kirby](#), The White House (2022).

13 Alex Young, [Too Much Information: Ineffective Intelligence Collection](#), Harvard International Review (2019); Cortney Weinbaum & John N.T. Shanahan, [Intelligence in a Data-Driven Age](#), Joint Force Quarterly (2018).

14 Tomas Chamorro-Premuzic, et al., [As AI Makes More Decisions, the Nature of Leadership Will Change](#), Harvard Business Review (2018).

AI and emerging technologies, and their limitations, to maximize the opportunities the technology can offer. To achieve this, promotion within the senior executive service ranks should require executive education on AI and emerging technologies.¹⁵

The Director for National Intelligence (DNI), Undersecretary of Defense for Intelligence, and the directors of Central Intelligence Agency, Defense Intelligence Agency, National Geospatial Agency, National Reconnaissance Office, and National Security Agency, in particular, must take the lead because their agencies are well-equipped to serve national missions. They are also uniquely positioned to lead their own staff and agency in transforming the bureaucracy.

IC leaders and their designated technology leadership should prioritize projects that **build internal tech expertise, improve data standardization and architecture, and support emerging tech adoption at scale across the IC.**

Creating a technology-enabled and AI-driven IC will need to be a community-wide effort. Over the years, the IC has developed several AI strategies and implementation plans,¹⁶ but they have been unevenly implemented across the community and individual agencies. The IC needs a single, cohesive strategy for transformation to turn isolated initiatives into a community-wide technological revolution. IC leaders and their designated technology leadership should prioritize projects that build internal tech expertise, improve data standardization and architecture, and support emerging tech adoption at scale across the IC.

Successful, at-scale digital transformation requires the right combination of people, processes, and technology. The IC requires a broad foundation to ensure that emerging technology services can be built, scaled, and effectively employed across mission areas. It needs people with the right expertise to advance technology; processes to manage areas where humans and technologies converge; and the right technology to store, process, and move data at immense scale. Integrating these elements is a challenge for any large enterprise, upsetting traditional career paths, workflows, data management, and technology integration. Shifting the IC's practices will require standardizing and contextualizing data for broader use, building a new digital backbone, and accessing

¹⁵ Andrew Ng, [AI Transformation Playbook](#), Landing AI (2020).

¹⁶ See e.g., [The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines](#), Office of the Director of National Intelligence (2019); [NGA Releases New Data Strategy to Navigate Digital](#), GEOINT Revolution, National Geospatial-Intelligence Agency (2021).

necessary talent. As these elements come together, the IC would gain agility and efficiency in iterating on existing applications and applying them to new problems.

To effectively counter adversaries and maximize the Intelligence Community's potential, U.S. intelligence and its external stakeholders must refine their sense of risk. Avoiding risks in the short term is a sure way of creating long-term risks for intelligence failures. As the speed of information, technological innovation, and decision-making accelerate, the IC should reevaluate the risk across all aspects of the enterprise — including how data is shared, how technology is acquired, and how talent is recruited. It also must include the risk of incremental changes or doing nothing. Sometimes, doing nothing can be the riskiest choice of all. Internally, this includes providing space for experimentation, tolerating failures, and ensuring that security practices support the intelligence mission. Externally, the IC must partner with Congress and the Administration so that external stakeholders accept reasonable risk-taking.

Building the conditions for a tech-enabled Intelligence Community also requires new security approaches that bring critical expertise and technology into the community. The IC has an opportunity to update its security practices and redefine the meaning of successful security. Success should be the safe employment of people and technology needed to execute its digital age mission facing an all-domain rival. Current security practices prevent many qualified candidates that have lived in the PRC from working in the IC.¹⁷ These security practices also slow down the adoption of needed, advanced commercial technology in favor of retaining older, government-approved technology.¹⁸ The IC needs dynamic, digital age-aware security practices that are fully aligned with overall national security and IC objectives.

U.S. intelligence leadership needs to revisit security processes and the preoccupation with counterintelligence risk minimization. Risks cannot be avoided in the world in which the IC is operating. Attempting to do so places barriers between U.S. intelligence and the resources, both human and technological, needed to adapt to the rivalry with the PRC and the digital era. The current security system was originally constructed to address threats against IC interests that exploited relatively small, stable, and predictable attack surfaces. The individualization of data, mobile telecommunication, social media, and the centralization of personal information on databases creates opportunities for hostile

¹⁷ [Promoting Cultural Diversity in the Intelligence Community: Recruiting and Clearing Personnel with Foreign Ties](#), Intelligence and National Security Alliance (2022); [The China Deep Dive: A Report on the Intelligence Community's Capabilities and Competencies with Respect to the People's Republic of China](#), House Permanent Select Committee on Intelligence at 28 (2020); Kenneth Lieberthal, [The U.S. Intelligence Community and Foreign Policy: Getting Analysis Right](#), Brookings at 32-33 (2009).

¹⁸ Emily Harding, [Move Over JARVIS, Meet OSCAR](#), Center for Strategic and International Studies at 2 (2022).

intelligence services to target IC employees and contractors without ever coming face to face with the individual.¹⁹ The attack surfaces that security now seeks to protect are constantly expanding and evolving in unpredictable ways.²⁰ Yet, the fundamentals of how people and technology are cleared have not significantly changed in decades.²¹

Accessing tech-savvy talent requires the Intelligence Community to adopt more flexible approaches for hiring and retention. The IC possesses three advantages over the private sector that ensure people will want to join, and even return, to public service. The first is a sense of purpose. The second is a unique problem set. The third is a sense of stability. However, the IC – and the U.S. Government more broadly – will continue to be challenged to compete directly with the private sector for compensation. Salaries for AI talent, in particular, continue to rise along with the demand in the private sector. The competition for technical expertise in the current market puts the IC at a disadvantage in hiring top-level talent.²² Beyond this technical talent, the IC also needs people adept at shaping how the community manages AI and other emerging technologies.

More flexible approaches to recruitment and career development would allow the IC to better harness expertise and stay at the cutting edge of technological development. The current personnel system generally does not reward individuals who move between the private sector and the IC. This internal orientation was less of a problem when significant technological innovation occurred inside the government, but the private sector has taken the lead in emerging technologies.²³ Only by allowing or facilitating government employees to move in and out of government or by developing personnel exchange or fellowship programs with the private sector will the IC ensure it has regular access to talent knowledgeable and capable of applying leading technologies. The National Reserve Digital Corps, proposed by the National Security Commission on Artificial Intelligence,

19 Digitalization of data and the spread of computers expanded the potential attack vectors again and the ability to identify who and where someone was. See Warren Strobel, [Biometrics, Smartphones, Surveillance Cameras Pose New Obstacles for U.S. Spies](#), Wall Street Journal (2021); Hardware vulnerabilities were joined by software vulnerabilities. More and more equipment and software used by the government were commercial off-the-shelf (COTS) products – all of which could be exploited directly or through supporting services and the supply chain. See e.g., [ASUS Software Updates Used for Supply Chain Attacks](#), Symantec Security (2019); Dina Temple-Raston, [A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack](#), NPR (2021).

20 Corin Stone, [Artificial Intelligence in the Intelligence Community: Money is Not Enough](#), Just Security (2021); Robert Wallace & H. Keith Melton, [Spycraft: The Secret History of the CIA's Spytechs, from Communism to Al-Qaeda](#), Plume at 223 (2008).

21 David Luckey, et al., [Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved?](#), RAND Corporation (2019).

22 Cade Metz, [A.I. Researchers Are Making More Than \\$1 Million, Even at a Nonprofit](#), New York Times (2018); The Senior Executive Service pay scale by contrast, tops out at \$226,300. See [Salary Table No. 2022-EX](#), U.S. Office of Personnel Management (2022).

23 Zachary Arnold, et al., [Tracking AI Investment: Initial Findings From the Private Markets](#), Center for Security and Emerging Technology (2020).

could enable this exchange.²⁴ Yet another talent pipeline for the IC could be a potential U.S. Digital Service Academy, also proposed by the NSCAI.²⁵

As it embraces AI, the Intelligence Community can learn from other complex organizations, while adapting the lessons to its specialized missions. Large, complex companies across a range of industries and employing tens of thousands of people have moved from the industrial age to the digital age by integrating AI and other emerging technologies throughout their operations. The IC has a unique mission and may have unique features, but some of the core principles for digital transformation appear consistent and can be adapted and leveraged to the IC's needs. These principles include a commitment from leadership, integrated digital infrastructure, and organizational capacity – all developed and applied in stages over time. But the private sector also provides negative examples of how AI initiatives fail. By treating digital transformation as a series of disconnected, independent experiments, rather than a disciplined, multi-stage process, organizations set themselves up for failure.²⁶

Beginning with a focused leadership aligned behind a single strategy for digital transformation, U.S. intelligence should progressively move its people, processes, and technologies through a series of phases.²⁷

The DNI should sponsor the creation of a Digital Experimentation and Transformation Unit to run pilot projects that address community-wide challenges on talent, processes, technologies, or acquisition as identified by the DNI and IC agency directors. The unit should be sponsored and empowered by the DNI, with one of the intelligence agencies serving as the executive agent, and with representatives from each member of the intelligence community. The purpose would be to identify and apply the best available technology and expertise in the United States to select community-wide problems. The DNI would also need support from Congressional appropriators to ensure the office has the necessary time and support to solve the selected problems. The pilot projects should address a key aspect of the people, processes, technology, and acquisition needs of the IC to accelerate its digital transformation. All projects would need to include programmatic analysis for

²⁴ The National Reserve Digital Corps, as envisioned by the NSCAI, would bring in digital expertise as civilian special government employees (SGEs) to work at least 38 days each year in government. The military reserves' service commitments and incentive structure would serve as the program's model. See [Final Report](#), National Security Commission on Artificial Intelligence at 10, 358–362 (2021).

²⁵ [Final Report](#), National Security Commission on Artificial Intelligence at 127 (2021). For additional detail on technology talent pipelines for the U.S. Government, see Chapter 2 of this Report.

²⁶ Andrew Ng, [AI Transformation Playbook](#), Landing AI (2020).

²⁷ The phases outlined below are drawn from a number of sources, including, SCSP Staff Engagement with AI business expert; Tomas Chamorro-Premuzic, et al., [As AI Makes More Decisions, the Nature of Leadership Will Change](#), Harvard Business Review (2018); Andrew Ng, [AI Transformation Playbook](#), Landing AI (2020); Manasi Vartak, [How to Scale AI in Your Organization](#), Harvard Business Review (2022).

each participating IC element to ensure successful projects are sustained beyond the new unit. The initial focus areas could include:

- The recruitment, vetting, and employment of personnel that possess needed expertise and/or meet some high-risk criteria;
- The improvement of systems interoperability across the IC; or
- The automation of cross-collection platforms tipping and queuing at the edge to improve IC indications and warning capabilities.

Leveraging Open Source Capabilities

In an age where most data resides in the open world,²⁸ the IC risks surprise and intelligence failure without a robust open source intelligence capability. The exponential growth in publicly and commercially available information has outpaced the IC's capability, or anyone's for that matter, to fully harness open source in support of U.S. decision making and policy.²⁹ This has come on top of the decline in the collection, processing, and usage of open source materials through the evolution of IC open source initiatives from the Foreign Broadcast Information Service (FBIS) to the Open Source Center to the Open Source Enterprise (OSE). Moreover, less attention to collection, user-unfriendly platforms, and overzealous security practices have limited U.S. intelligence analysts' effective access to and use of government open source resources over time.³⁰

To be sure, there are no substitutes for U.S. eyes and ears inside the hallways of foreign capitals. However, the integration of open source data as part of an automated intelligence cycle could enable and focus clandestine intelligence collection on the most important collection targets. Moreover, machine learning models can be employed to label, classify, cluster, and connect data to publicly validate U.S. claims about the malign activities of the PRC and Russia without compromising the IC's sources and methods.

The U.S. Government must address this and build a tech-enabled open source entity, particularly one with the potential to drive speed of execution, experimentation, and collaboration.

28 The International Data Corporation estimated that the amount of data in the world would increase from 33 Zettabytes (ZB) in 2018 to 175 ZB by 2025. One ZB is one trillion gigabytes. See David Reinsel et al., [The Digitization of the World from Edge to Core](#). International Data Corporation at 7 (2018).

29 [Report to the President of the United States](#), The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction at 23, 377-380 (2005); Heather J. Williams & Ilana Blum, [Defining Second Generation Open Source Intelligence \(OSINT\) for the Defense Enterprise](#). RAND Corporation (2018); Cortney Weinbaum, et al., [Options for Strengthening All-Source Intelligence: Substantive Change Is Within Reach](#), RAND Corporation (2022).

30 SCSP staff engagement with open source experts (June 2022).

The U.S. Government must place the collection of publicly available information, acquisition of commercially available information, and their processing at the center of its renewed open source efforts. Calls for an effective open source entity date back to the Cold War.³¹ IC experts have long estimated that over 80 percent of the information needed to support intelligence, military operations, public diplomacy, and other policy initiatives can be acquired publicly or commercially.³² As the potential of publicly available information grew well beyond print and broadcast media, so too did the calls for improvements to the IC's open source capabilities.³³ In more recent years, independent commissions and various studies have reiterated these calls. In 2005, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction stated "The Intelligence Community does not have an entity that collects, processes, and makes available to analysts the mass of open source information that is available in the world today."³⁴ Subsequent studies of open source intelligence have reinforced the need for a central entity within the Intelligence Community or U.S. Government.³⁵ While calls for an open source organization are not new, the United States can no longer ignore the value of publicly and commercially available information; the urgency of the techno-economic competition demands action immediately.

A necessary first step in harnessing the potential of open source data is for all the U.S. Government departments and agencies to significantly improve their sharing of information with one another, which is something that the current *Federal Data Strategy* already encourages.³⁶ But the other critically important step is for the IC, and even more broadly, the U.S. Government to address the collection, acquisition, and processing of foreign publicly and commercially available information.

The U.S. Government should create a new, well-resourced institutional home for open source collection, acquisition, processing, and analysis. The difficulties and costs of collecting open source data, the specialized skills required to handle such data, and privacy

31 Herman L. Croom, [The Exploitation of Foreign Open Sources](#), Studies in Intelligence (1969).

32 Herman L. Croom, [The Exploitation of Foreign Open Sources](#), Studies in Intelligence (1969); Richard A. Best Jr. & Alfred Cumming, [Open Source Intelligence \(OSINT\) Issues for Congress](#), Congressional Research Service at 4 (2007); Anthony Olcott, [Open Source Intelligence in a Networked World](#), Bloomsbury at 17 (2014).

33 [Preparing for the 21st Century: An Appraisal of U.S. Intelligence](#), Commission on the Roles and Capabilities of the United States Intelligence Community at xxi, 88-89 (1996); [Roadmap for National Security: Imperative for Change](#), U.S. Commission on National Security/21st Century at xiv (2001).

34 [Report to the President of the United States](#), The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction at 23 (2005).

35 Heather J. Williams & Ilana Blum, [Defining Second Generation Open Source Intelligence \(OSINT\) for the Defense Enterprise](#), RAND Corporation (2018); Cortney Weinbaum, et al., [Options for Strengthening All-Source Intelligence: Substantive Change Is Within Reach](#), RAND Corporation (2022).

36 [Federal Data Strategy](#), Office of Management and Budget (last accessed 2022).

concerns related to some of the data suggest that this mission can only be addressed by an entity tailored for the task. A clear institutional home would also provide clarity of purpose and mission focus.

As foreign targets learn how researchers or governments might exploit publicly available information to inform future policy actions, they can be expected to adjust and adapt their activities accordingly – changing URLs, putting access controls in place, altering content, or even removing it entirely.³⁷ The U.S. Government needs to position itself now to exploit such closing windows of opportunity. With U.S. rivals also increasingly aware of what open source researchers are doing online and the potential policy consequences of such research,³⁸ professional tradecraft is more frequently needed to access quality open source information across barriers put up by rivals, such as requirements for true names, local phone numbers, and official identification numbers.³⁹

Normalizing the use of open sources among all-source analysts does not address this problem. Those analysts, whose expertise lies in a regional or functional specialty and supporting decisions, cannot replace the role of dedicated collectors.⁴⁰ Furthermore, the procurement and collection of publicly and commercially available information demands a cadre of professional collectors with both domain expertise and technical knowledge to discern credible sources from those that are not, and to communicate the necessary context as open source reports are disseminated for wider usage.

Finally, the cost and privacy concerns associated with commercially available information require deliberate acquisition and management efforts. Private companies now have their own sensors. They collect digital data on a range of relevant economic and human activities. Such data, however, is not free. More importantly, it can include information on U.S. persons, necessitating careful handling to protect their privacy and to ensure that agencies receive only the data they are allowed to receive.

37 SCSP Open Source Working Group (February 2022); Stephanie Yang, [As China Shuts Out the World, Internet Access from Abroad Gets Harder Too](#), LA Times (2022); Sébastien Seibt, [China's Data 'Disappearance' Makes Information Access Rough Going for Outsiders](#), France 24 (2021); Glenn D. Tiffert, [Peering down the Memory Hole: Censorship, Digitization, and the Fragility of Our Knowledge Base](#), The American Historical Review (2019).

38 Sébastien Seibt, [China's Data 'Disappearance' Makes Information Access Rough Going for Outsiders](#), France 24 (2021); Luo Jiajun & Thomas Kellogg, [Verdicts from China's Courts Used to Be Accessible Online. Now They're Disappearing.](#), ChinaFile (2022).

39 Josh Chin, [China Is Requiring People to Register Real Names for Some Internet Services](#), Wall Street Journal (2015).

40 Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, [Using Open Source Information Effectively](#) at 31 (2005).

Options for Leveraging Open Source Capabilities

	Option 1: New Open Source Information Agency (Outside the IC)	Option 2: New Open Source Intelligence Agency (Within the IC)	Option 3: New ODNI Open Source Coordination Office (OSCO)	Option 4: Normalize Open Source Use Across IC Analytic Units
Brief Description	Establish an independent agency or office to carry out open source analysis and informational support for U.S. policymakers and the IC.	Establish an independent agency primarily responsible for the collection and analysis of open source intelligence.	Establish an office within the ODNI that would host open source information for the IC. OSCO would serve as the IC's focal point for open source contracting and processing.	Encourage the normalization of open source in the IC by creating an set of standards when collecting, processing, and analyzing open source data.
Institutional Location	Potential locations include: - Executive, Standalone Agency - Commerce, Independent Office - Defense, Independent Agency - State, Independent Office - GSA, Independent Office-	19th Member of the IC.	ODNI	Across IC elements
Legal Authority to Access and Acquire Data	While this agency is not limited by Title 50 authorities, its collection activities will be governed by the existing or future statutory schemes consistent with the broad policy objectives of its host agency or branch.	This agency would be subject to Title 50 authorities. However, the DNI should further designate it as the IC agency responsible for the collection of open source intelligence within the Title 50 framework.	This office would be subject to Title 50 authorities. However, ODNI must also pursue blank purchase agreements within the 48 CFR § 8.405-3 framework.	Authorities would vary based on the agency implementing the policies.
Oversight and Accountability	Subject to congressional oversight by the relevant committees and/or jointly with SSCI & HPSCI, with any other form of oversight varying based on the selected host agency.	Subject to congressional committee oversight (SSCI & HPSCI). Additional interactions from governing board and an advisory committee.	Subject to congressional committee oversight (SSCI & HPSCI).	Subject to congressional committee oversight (SSCI & HPSCI), with any other form of oversight varying based on the agency.
Pros	<ul style="list-style-type: none"> • Lower barriers for entry with personnel, partnerships, and technology. • More likely to operate at lowest level of classification. 	<ul style="list-style-type: none"> • Legitimizes OSINT as IC function. • Benefits from existing IC budget and infrastructure. 	<ul style="list-style-type: none"> • Resolves the acquisition problem for commercially available data. • Centralizes publicly/commercially available data within the IC. 	<ul style="list-style-type: none"> • Intelligence agencies have autonomy to meet their own open source needs. • Requires no action from outside the IC.
Cons	<ul style="list-style-type: none"> • Limits potential impact on IC. • Standing up an entity takes time. 	<ul style="list-style-type: none"> • Requires new legislation. • Standing up an agency takes time. 	<ul style="list-style-type: none"> • Retains the status quo for all-source analysis. • Relies on outsourced expertise. 	<ul style="list-style-type: none"> • This is the status quo. • Open source collection and processing problems remain unresolved.

The U.S. Government has a number of options to choose from on how to stand up an open source entity. While the precise organizational model for an open source entity is secondary to ensuring that it meets the U.S. Government's needs, there are several options to choose from to address the imperative of the open source mission. In assessing the various options, U.S. Government stakeholders should be mindful of several attributes that could make such an open source entity a success: (1) It should be connected to and have a voice within the IC, regardless of where it sits; (2) It should have a hybrid workforce, including cleared and uncleared personnel, and develop expertise through time on target and promotions; (3) It should have a clear collection and processing mission; (4) It should serve as a focal point for U.S. Government absorption and integration of commercially available data; (5) Other IC agencies and the U.S. Government, more generally, should be able to access, search, and use this data for their own queries and AI projects; (6) Such an entity should also serve as a gateway through which nongovernmental analysts, academic researchers, and the public writ large could access open source information; and (7) It should be able to liaise with counterparts among allies and partners.

This entity could be organized in one of three broad ways. The first is as an independent agency within the executive branch, either as an independent office reporting to the White House or an agency reporting to an existing department. Potential departments include the Departments of State, Defense, Commerce, or the General Services Administration. The second way is as an IC entity, its 19th member, primarily responsible for the collection and analysis of open source intelligence. The third way is a coordinating office within the Office of the Director of National Intelligence that would host open source information for the IC, deconflict the IC's open source activities, coordinate purchasing, licensing, and managing of commercial data for the U.S. Government, and serve as a point of contact for the external open source research community. One final option would not rely on establishing a new entity; rather, it would entail the methodical integration of open sources in greater quantities in all-source analysis and the creation of a set of standards when collecting, processing, and analyzing open source data. This option would likely require changes to analytic training and tradecraft, review processes, and resources.⁴¹

⁴¹ For the most technology savvy version of this argument, see Emily Harding, [Move Over JARVIS, Meet OSCAR](#), Center for Strategic and International Studies (2022).

Strengthening U.S. open source capabilities provides one of the best “use cases” for shifting the IC practices critical to mastering artificial intelligence. In strengthening open source, the IC could also make it into the leading “use case” for AI-enabled transformation because:

- The ability to transfer commercial AI approaches to open source problems would streamline its path to success and allow an open source entity to become operational and scale faster.
- The demand for open source intelligence is profound, and multiple agencies can leverage open source data for their own insights. Using AI would enable the curation and improved vetting of open source data at scale.
- The relative transparency of an open source agency would ensure that AI and emerging technologies achievements and lessons learned would remain visible to other individual agencies and help guide them in their own technology transformation. The current pedagogical approach of learning from intelligence failures and keeping successes secret is inadequate in the age of AI and emerging technologies.

As part of the transition toward a new, open source entity, all-source analytic units should run a series of internal pilot projects to build skills in exploiting open sources with AI tools. Open source analysts must tackle the same intelligence topics as collectors and analysts within other intelligence disciplines to be taken seriously. Individual IC entities should establish AI-empowered red teams composed of open source analysts to assess publicly and commercially available data for comparison with classified products. Pilot red teams would provide an opportunity to train open source analysts on AI tools, and simultaneously demonstrate the utility of both AI and open source data to intelligence analysis writ-large.

These pilot projects should be explicitly designed to complement an overarching strategy that aims to catalyze the Intelligence Community’s transition into a modern enterprise with expertise in all intelligence disciplines – including open source. Without a broader plan, such projects could end without a measurable impact on the wider U.S. intelligence enterprise, as occurred with experimental projects like Open Source Works.⁴²

The U.S. Government must attempt to make select open source products a utility available to all Americans, creating a virtuous cycle of expertise between government and non-

⁴² Open Source Works was a small CIA unit with roughly 100 analysts who had exceptional language skills but did not have security clearances. Experienced analysts, who held security clearances, helped guide their open source collection and analysis, so that it was relevant for CIA and the U.S. Government. SCSP Staff Engagement with Retired Intelligence Official (March 2022); Gregory F. Treverton, [Agenda for the Director of National Intelligence](#), SMA (2021).

government experts. The intensity and stakes of the current techno-economic competition require a higher degree of shared knowledge and understanding across U.S. society. The opaque and controlled information environments of U.S. rivals, especially the PRC, require a high degree of knowledge to identify the authoritative signals that these governments publish for internal and external audiences. From the 1940s to 2013, when the service ended, IC open source experts helped curate and publish foreign media translations and analyses for public use.⁴³ U.S. academics, in turn, used these resources – often not readily available elsewhere – to shed light on important developments in the PRC and other closed societies, which in turn informed U.S. policymakers. The U.S.

The intensity and stakes of the current techno-economic competition require a **higher degree of shared knowledge and understanding** across U.S. society.

Government should recreate this service for an age of AI and emerging technologies. It must treat open source as a utility that enables the IC's ability to provide insight to Americans outside of government and harness insights from these Americans to inform policymakers.

Creating Techno-Economic Intelligence

U.S. intelligence capabilities are pivoting toward the bipartisan U.S. policy statement that “economic security is national security.”⁴⁴ U.S. intelligence must retool for economic competition in order to defend Americans’ standard-of-living, support a U.S. Techno-Industrial Strategy,⁴⁵ and protect the interests of the United States and its allies around the world. This re-tooling should be based on an initial net characterization of the techno-economic competition with China.

43 At the end of 2013, OSC shut down the subscription service, citing costs, the availability of alternative sources, and potential copyright issues. See Steven Aftergood, [CIA Halts Public Access to Open Source Service](#), Federation of American Scientists (2013); Steven Aftergood, [CIA Cuts Off Public Access to Its Translated News Reports](#), Federation of American Scientists (2014); Steven Aftergood, [Open Source Center \(OSC\) Becomes Open Source Enterprise \(OSE\)](#), Federation of American Scientists (2015).

44 [Interim National Security Strategic Guidance](#), The White House (2021); [U.S. National Security Strategy](#), The White House (2017); The IC has taken steps to add leadership in this area: in 2020, the DNI established the role of Economic Security and Financial Intelligence Executive (EFX), who reports to the Deputy Director, Mission Integration. The EFX is responsible for “interagency and foreign partnership activities related to economic security, energy security, export controls, investment security, sanctions, supply chain, telecommunications, threat finance, and trade.” [President Biden Announces Key National Security Nominations](#), The White House (2021); [Additional Pre-Hearing Questions for Ms. Shannon Corless upon her nomination to be Assistant Secretary for Intelligence and Analysis, Department of the Treasury](#), United States Senate Select Committee on Intelligence at 4 (2021).

45 For more on a Techno-Industrial Strategy, see Chapter 2 of this report.

U.S. intelligence should leverage insights from the private sector to improve the picture of U.S. adversaries' economic, financial, and technological capabilities. U.S. intelligence should leverage, not recreate, the private sector's collection and analysis of economic information. Forming public-private partnerships with industry, Wall Street banks, consulting firms, academia, and the business media would enable U.S. intelligence to efficiently build upon their sector expertise, broader resources, on-the-ground presence, and market-based insights, and marry them with IC information to create a more comprehensive intelligence picture. The Department of Commerce, in particular, should expand its techno-economic intelligence capabilities and set up an office responsible for fusing industry data already collected by Commerce with U.S. intelligence reporting to produce sector-specific techno-economic threat intelligence for industry and policymakers, while ensuring the necessary safeguards to protect the privacy of American citizens and proprietary information of U.S. companies.

The U.S. Government should establish a National Techno-Economic Intelligence Center. The U.S. Government should create a National Techno-Economic Intelligence Center that can coordinate economic threat information and work closely with policymakers on responses to these threats.⁴⁶ The center should be established under a well-resourced sponsor that can support its mandate within government. Using AI to collect and process economic information at scale, this economic "nerve center" would be able to make economic assessments and forecasts and fuel innovation in economic modeling. This center, with analysts trained for techno-economic analysis, would warn of U.S. economic vulnerabilities, make sense of rivals' grand strategies,⁴⁷ send warnings to U.S. industry about economic threats, especially intellectual property theft, and evaluate opportunities to deploy tools of economic leverage.

U.S. intelligence needs the authorities, capabilities, and incentives to make techno-economic net assessments. The IC should be able to provide policymakers with an economic "order of battle" for our strategic rivals that maps out and details critical supply chains, technologies, industries, and companies. U.S. intelligence needs the authority and internal guidelines to conduct these net assessments informed by an awareness of the U.S. techno-economic landscape⁴⁸ while ensuring appropriate privacy safeguards for U.S. citizens. It should prioritize supporting other government centers tasked with providing technology

46 Anthony Vinci, [Competitive Climate: America Must Counter China by Investing in Economic Intelligence](#), National Interest (2020); John Costello, et al., [From Plan to Action: Operationalizing a U.S. National Technology Strategy](#), Center for a New American Security (2021).

47 Rush Doshi, [The Long Game: China's Grand Strategy to Displace American Order](#) (2021).

48 The IC has taken initial steps in this direction: in 2019, ODNI established the Office of IC Net Assessment to "assess what other intelligence agencies around the world are doing and why, what the most effective technologies will be to cope with those changes, and how the world is changing strategically." Colin Clark, [IC Net Assessment: Interview With Director Flynn](#), Breaking Defense (2019).

net assessments, such as the Office of Global Technology Competition Analysis proposed by the American Technology Leadership Act⁴⁹ (and included in the Senate version of the Intelligence Authorization Act for FY2023)⁵⁰ or a Technology Competitiveness Council (TCC) proposed in Chapter 1 of this report.

U.S. intelligence collection should include adversary scientific and technological research that has dual-use purpose or application. The United States has enjoyed the position as the world's dominant economic and technological power since World War II,⁵¹ reducing somewhat the need for IC awareness of adversarial scientific and technological research. However, growing research on dual-use technologies and their applications by U.S. adversaries that leverages innovations across military and civilian sectors requires the IC to expand its awareness.⁵² For example, the PRC's economic growth over the last 40 years has brought it to a peer or near-peer status in a number of critical technologies, such as computer vision, next-generation mobile communications, and battery technology.⁵³ The PRC's national strategy for military-civil fusion, through which it integrates its civilian economy with its military industrial base, underscores that techno-economic competition carries directly over into traditional national security areas.⁵⁴ The PRC's domestic innovation base,⁵⁵ aided through its theft of U.S. intellectual property,⁵⁶ should be considered a U.S. intelligence collection priority, which can be employed to inform our own, government-led scientific and technological research efforts.

Countering Foreign Adversarial Influence Operations

U.S. rivals increasingly resort to the aggressive use of disinformation to target U.S. decision-making, reputation abroad, and social cohesion at home. Trolls, bots, and deepfakes deployed by the PRC's cyber militias and Russia's Internet Research Agency are also aiming at incremental erosion of key tenets of democracy until people question what is

49 [Bennet, Sasse, Warner Unveil Legislation to Strengthen U.S. Technology Competitiveness](#), Senator Michael Bennet (2022).

50 S. 4503, [Intelligence Authorization Act for Fiscal Year 2023](#) (2022).

51 Fareed Zakaria, [The Future of American Power: How America Can Survive the Rise of the Rest](#), Foreign Affairs (2008).

52 [Annual Report to Congress: Military and Security Developments Involving the People's Republic of China](#), Office of the Secretary of Defense at IV (2021).

53 [Final Report](#), National Security Commission on AI at 161 (2021); Dennis Normile, [A Beijing Think Tank Offered a Frank Review of China's Technological Weaknesses. Then the Report Disappeared](#), Science (2022); Martin Placek, [Share of the Global Lithium-Ion Battery Manufacturing Capacity in 2021 with a Forecast for 2025, by Country](#), Statista (2022); Govind Bhutada, [Mapped: EV Battery Manufacturing Capacity, by Region](#), Visual Capitalist (2022); [Lithium-ion Battery Market Size Worth \\$182.53 Billion By 2030: Grand View Research, Inc.](#), Bloomberg (2022).

54 [Military-Civil Fusion and the People's Republic of China](#), U.S. State Department (2020).

55 Emily S. Weinstein, [Beijing's 're-innovation' Strategy is Key Element of U.S.-China Competition](#), Brookings (2022).

56 [Remarks by FBI Director Wray on The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States](#), Hudson Institute (2020).

demonstrably true.⁵⁷ The acceleration of technological advancements and the emergence of new media platforms have enhanced the speed, reach, volume, and precision of disinformation generated by foreign adversaries. The scale, scope, and snowballing effect of these influence operations make disinformation a particularly acute concern for

The acceleration of technological advancements and the emergence of new media platforms have enhanced the **speed, reach, volume, and precision of disinformation** generated by foreign adversaries.

national security. The U.S. Government must protect Americans from, counter the effects of, and disrupt adversary influence operations.

The U.S. Government – including the Intelligence Community – must counter foreign adversarial influence operations through early-stage countermeasures. Prior to Russia’s invasion of Ukraine, the United States and the United Kingdom engaged in what appears to have been deliberate disclosure and exposure of Russian malign intentions.⁵⁸ This approach should be replicated whenever possible and suitable. Through early disclosures

of anticipated physical or virtual malign actions, U.S. and allied governments could potentially deter or, at a minimum, “prebunk” them.⁵⁹ The “prebunking” could help raise awareness among the domestic public, enabling them to sense and avoid misleading content proliferating in their newsfeeds.⁶⁰

But deterrence-related and “prebunking” disclosures may not always be possible.⁶¹ The U.S. Government should also aim to identify and alert the public of foreign disinformation operations that seek to undermine the social cohesion of the United States. While such disinformation operations may not have an obvious tactical urgency, they can have

57 Katerina Sedova, et al., [AI and the Future of Disinformation Campaigns Part 1: The RICHDATA Framework](#), Center for Security and Emerging Technology (2021); Katerina Sedova, et al., [AI and the Future of Disinformation Campaigns Part 2: A Threat Model](#), Center for Security and Emerging Technology (2021).

58 Jessica Brandt, [Preempting Putin: Washington’s Campaign of Intelligence Disclosures is Complicating Moscow’s Plans for Ukraine](#), Brookings (2022); Douglas London, [To Reveal, or Not to Reveal: The Calculus Behind U.S. Intelligence Disclosures](#), Foreign Affairs (2022).

59 Laura Garcia & Tommy Shane, [A Guide to Prebunking: A Promising Way to Inoculate Against Misinformation](#), First Draft (2021).

60 Jon Roozenbeel, et al., [Prebunking Interventions Based on “Inoculation” Theory Can Reduce Susceptibility to Misinformation Across Cultures](#), Harvard Kennedy School Misinformation Review (2020); Jonas De keersmaecker & Arne Roets, [“Fake News”: Incorrect, but Hard to Correct. The Role of Cognitive Ability on the Impact of False Information on Social Impressions](#), *Intelligence* at 65, 107-110 (2017).

61 Simge Andi & Jesper Akesson, [Nudging Away False News: Evidence from a Social Norms Experiment](#), *Digital Journalism* at 121 (2020).



Sources:
 Laura Garcia & Tommy Shane, A Guide to Prebunking: A Promising Way to Inoculate Against Misinformation, First Draft News (2021).
 Fact-Checking and Debunking: A Best Practice Guide to Dealing with Disinformation, NATO Strategic Communications Center of Excellence (2021).

strategic consequences. The IC entities could collaborate on this endeavor with the Cybersecurity and Infrastructure Security Agency (CISA) and expand the National Cyber Awareness System⁶² to potentially alert the public about foreign disinformation operations of strategic import.

Finally, the IC can also publicly identify false narratives and themes propagated by U.S. adversaries that aim at the truth more broadly and at U.S. reputation abroad. This

62 [National Cyber Awareness System](#), Cybersecurity & Infrastructure Security Agency (last accessed 2022).

publicizing could be done for the purpose of encouraging and enabling private sector and academic researchers to examine them further. Independent expertise could thus be a force multiplier for a resource-demanding mission.

Identify a focal point that tracks, counters, and disrupts foreign-directed denigration campaigns against senior civilian and military leaders. Our adversaries are working to acquire, analyze, and weaponize data on DNA, dating preferences, shopping tendencies, social networking, and professional experiences of much of the U.S. population.⁶³ Empowered by AI, this could allow foreign intelligence services to micro-target senior civilian and military leaders by denigrating them in the public domain and orchestrating character assassination efforts,⁶⁴ which would put such senior leaders under considerable pressure and distract them from discharging their duties. At present, it appears that no entity in the U.S. Government is specifically tasked and resourced to track, counter, and disrupt such denigration efforts – and the collection efforts that support them. While further analysis of authorities and broader engagement of various stakeholders is required to recommend an institutional home, the imperative for establishing or designating an entity that focuses on this mission is already here.

The constant evolution of influence operations requires the Intelligence Community – and U.S. Government writ large – to incorporate new technologies and mitigation techniques quickly. Digital influence operations advance at an exponential rate, presenting the IC with the challenge of keeping pace.⁶⁵ Leveraging tools like the content provenance standards of the Coalition for Content Provenance and Authenticity⁶⁶ and DeepMind’s RETRO database⁶⁷ could help the IC outpace adversaries by authenticating content origins and verifying information, respectfully, while embracing high speed human-machine teaming would increase overall speed of IC operations.⁶⁸

63 For further discussion on individualized micro-targeting, see Chapter 5 of this report.

64 One example abroad is the targeting of U.S. Foreign Service Officer Julie Eadeh in Hong Kong. Timothy McLaughlin, [How China Weaponized the Press](#), The Atlantic (2021). Note that micro-targeting is not limited to senior government civilian and military leaders, and also applies to kinetic attacks. For further discussion on micro-targeting, see Chapter 5 of this report.

65 Examples of recent developments include AI-enabled autonomous disinformation, texts produced by large language models, and realistic images produced by systems like [DALL-E 2](#), OpenAI (last accessed 2022).

66 [C2PA Specifications](#), Coalition for Content Provenance and Authenticity (2022).

67 Will Douglas Heaven, [DeepMind Says Its New Language Model Can Beat Others 25 Times Its Size](#), MIT Technology Review (2021).

68 For further discussion of Human-Machine Teaming in the defense context, see Chapter 5 of this report.

The Technologies That Will Drive Future American Competitiveness

Mid-Decade Challenges to National Competitiveness

07



• Artificial Intelligence

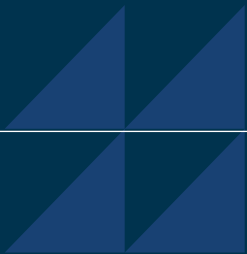
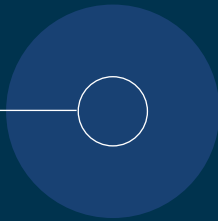
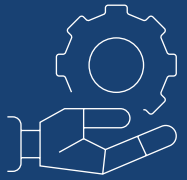
• Compute

• Networks

• Biotechnology

• Energy Generation and Storage

• Smart Manufacturing



CHAPTER 7

The Technologies That Will Drive Future American Competitiveness

Two multi-trillion dollar questions loom over the future of competition: which technologies will shape the destiny of nations, and how can America be poised to gain positional advantage in each destiny-shaping technology?

The innovations of the last two decades primarily unfolded in the digital realm. The next phase of technological innovation is an intersection of both emerging and evolving general purpose technologies (GPTs)¹ unfolding across three intersecting domains: *the physical (atoms), the digital (bits), and the biotechnical (cells)*.² GPTs, like electricity, support all aspects of modern society and usher in revolutions far beyond their initial technical

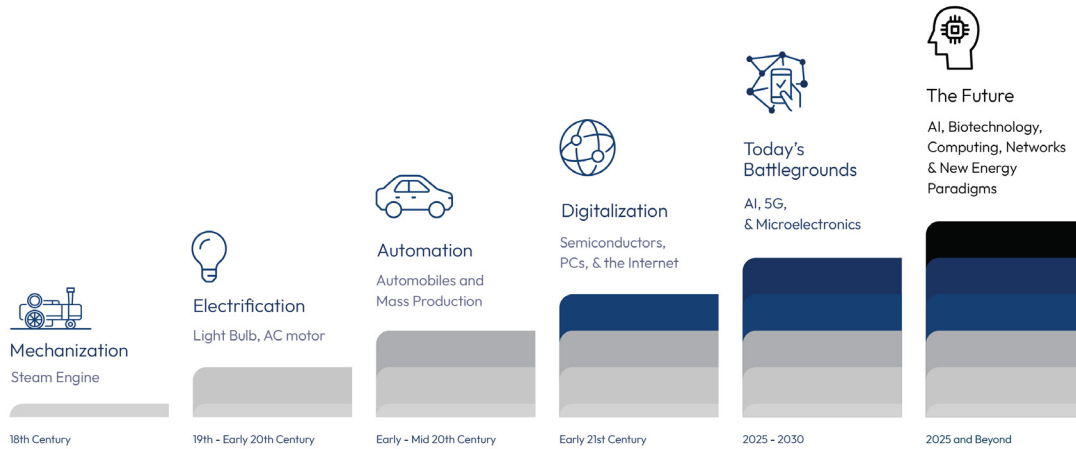
The next phase of technological innovation is an intersection of both emerging and evolving general purpose technologies (GPTs) unfolding across three intersecting domains: **the physical (atoms), the digital (bits), and the biotechnical (cells).**

1 No single definition of a GPT exists. Bresnahan and Trajtenberg in 1995 defined “general purpose technologies” as technologies that are characterized by their pervasiveness, inherent potential for technical improvements, and “innovational complementarities” that give rise to scale. Timothy F. Bresnahan & Manuel Trajtenberg, [General Purpose Technologies ‘Engines of Growth’](#), *Journal of Econometrics* (1995). Bekar, Carlaw, and Lipsey added additional criteria including that: a GPT has no substitutes, and downstream innovations enabled by a GPT would not have otherwise been possible. Clifford Bekar, et al., [General Purpose Technologies in Theory, Applications and Controversy: A Review](#), Simon Fraser University (2016).

2 “Atoms, bits, and cells” is a simple mnemonic we use to explain that the emerging and disruptive technologies of our day are touching the fundamentals of the physical (e.g. new metals), digital (e.g. new compute paradigms), and biological realms (e.g. new capabilities like CRISPR). Innovation is also increasingly crossing over in these domains such as DeepMind’s AlphaFold which predicts a protein’s 3D structure from its amino acid sequence. See [AlphaFold](#), DeepMind (last accessed 2022).

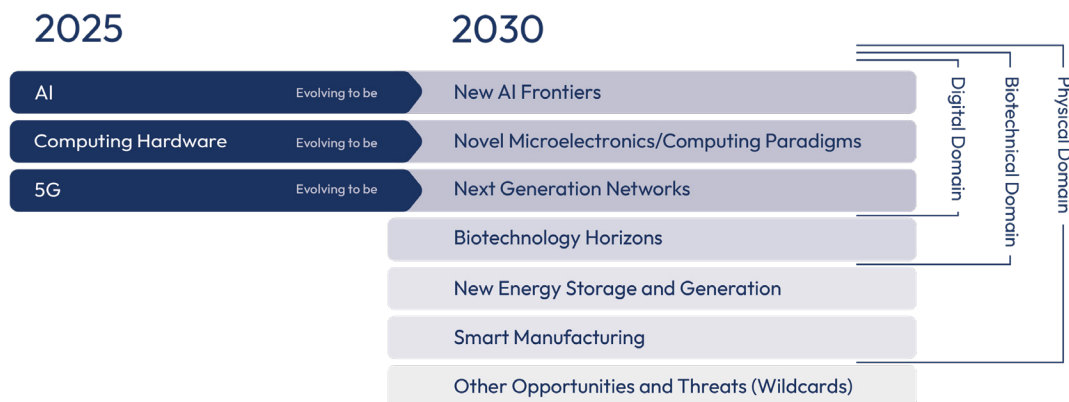
scope, driving economic growth for decades once they gain wide adoption. Looking out to 2025-2030, the competition over additional GPTs including biotechnology and new forms of energy generation, and areas where they converge like smart manufacturing, should be priorities requiring the United States to begin planning now.

Waves of General Purpose Technologies (GPTs)



This expansion of innovation portends a tectonic shift of the global geopolitical and economic status quo. Nations – especially China – are already trying to stake dominant positions in these century-shaping technologies. Positioning the United States for advantage in the GPTs of the 21st century will require investing not only in the research and development of these technologies, but also in bar-setting technology objectives to harness our public-private ecosystem and the resultant changes to improve our economy and society. With a growing number of complex issues demanding finite resources and leadership attention, the United States should prioritize and begin making the moves likely to serve as the foundations for subsequent step changes in the history of technology.³

³ For more information on a national process for technology competition, see Chapter 1 of this report.



The contours of 2030 technological leadership will likely flow from these five general purpose technologies — AI, compute, networks, biotechnology, energy storage/generation — and the convergence of these technologies, which manifests most apparently now in smart or advanced manufacturing. At the same time, other currently unforeseeable opportunities and threats could prove existential in this timeframe and require concerted national effort. In this chapter, we sketch some of the tech opportunities most apparent on the horizon that the United States should seize to ensure its long-term competitiveness.

Artificial Intelligence

AI sits at the center of a constellation of several emerging technologies and is increasingly driving progress in other fields. A few examples include its already-existent capacity for accelerating drug discovery,⁴ discovering new materials that will unlock new applications from chemistry to manufacturing,⁵ enabling autonomous vehicles to rapidly adapt to new environments,⁶ and controlling the plasma within a fusion device via deep reinforcement learning.⁷ Advances in large “foundation models” for both image generation and natural language processing continue to defy expectations,⁸ with recent models capable of generating accurate photorealistic images on demand.⁹ Researchers are already exploring

4 Ewen Callaway, [What's Next for AlphaFold and the AI Protein-Folding Revolution](#), Nature (2022).

5 Brian L. DeCost, et al., [Scientific AI in Materials Science: A Path to a Sustainable and Scalable Path](#), Machine Learning: Science and Technology (2020); Tom Fleischman, [AI Powers Autonomous Materials Discovery](#), Cornell Chronicle (2021).

6 Will Douglas Heaven, [The Big New Idea for Making Self-Driving Cars That Can Go Anywhere](#), MIT Technology Review (2022).

7 Jonas Degraeve, et al., [Magnetic Control of Tokamak Plasmas Through Deep Reinforcement Learning](#), Nature (2022).

8 [Huge “Foundation Models” Are Turbo-Charging AI Progress](#), The Economist (2022).

9 Sharan Narang & Aakanksha Chowdhery, [Pathways Language Model \(PaLM\): Scaling to 540 Billion Parameters for Breakthrough Performance](#), Google AI Blog (2022); Will Douglas Heaven, [This Horse-Riding Astronaut is a Milestone in AI's Journey to Make Sense of the World](#), MIT Technology Review (2022).

combining language models with computer vision to enable AI systems to not only recognize objects but also better infer context.¹⁰ Robotics will also benefit from improvements in AI advancements' ability to sense environments and make decisions.¹¹

U.S. leadership will entail not only continuing to ensure that American and partner-based entities are driving the frontier in AI research, but that those institutions are addressing the challenges of predictability and bias so that AI yields positive and inclusive outcomes. An example of a bold AI objective would be queryable AI systems that enable human users to better understand why an AI system made certain decisions, which could bolster trust in AI systems and also help humans detect and mitigate bias.¹² As the NSCAI noted, how AI systems reason remains a research frontier and such a goal could help accelerate progress in the field.¹³

LLMs “Ghost Chapter”

Artificial intelligence has advanced to the point where Large Language Models (LLMs) trained on portions of the Internet can coherently diagnose geopolitics and prescribe reasonably sensible policy recommendations. We asked three LLMs — OpenAI’s GPT-3, Hugging Face’s BLOOM, and a model developed by Anthropic — to answer some of the key questions that this report seeks to address. SCSP authors generated multiple responses to each question and selected the response that they judged most appropriately answered the question that was posed:

Is the United States or China winning the global techno-economic competition?

“China is giving the United States a run for its money in the global techno-economic competition. China is investing heavily in research and development, high-tech industries, and infrastructure, and it is quickly closing the gap with the United States in many areas of technology. However, the United States still maintains an edge overall with its leading universities and companies, entrepreneurial culture, openness to global talent, and strong investments in research and development. The global tech race between the

10 Kyle Wiggers, [Deep Science: Combining Vision and Language Could Be the Key to More Capable AI](#), TechCrunch (2022).

11 Teejay Boris, [This Robot Shapes Letters Using Play-Doh Like a Kid, Thanks to AI](#), TechTimes (2022).

12 For more information about mitigating bias in AI systems, see Chapter 3 of this report.

13 [Final Report](#), National Security Commission on Artificial Intelligence at 35 (2021).

two countries will likely remain fierce for many years to come.” — Anthropic¹⁴

Overall, what are the most important factors in the U.S.-China techno-economic competition today?

“Overall the most important factors in the U.S.-China techno-economic competition today are China’s economic transition, China’s increasing focus on its own innovation and science, the U.S.’ own transition toward more balanced innovation across its economy, and the U.S.’ growing need for high-tech equipment and systems. The U.S. remains an economic superpower and is the leading technology and innovation force in the world today. China is still far behind the U.S. in that regard and China is becoming a more significant competitor as it moves to fulfill its promise as the world’s leading country and power.” — BLOOM¹⁵

Which technologies will most significantly transform the economy, society, and national security between now and 2030?

“Between now and 2030, several technologies will likely most significantly transform the economy, society, and national security. These include artificial intelligence, robotics and automation, biotechnology and biomedicine, renewable energy, quantum computing, the Internet of Things, fifth-generation wireless networks or 5G, materials science, and autonomous vehicles. These technologies will drive dramatic gains in productivity and economic growth, revolutionize manufacturing and transportation, enhance human capabilities, and reshape the global balance of economic and military power.” — Anthropic¹⁶

How should a nation judge which technologies will be future geopolitical battlegrounds?

“The United States has been a world leader in technology for decades, but the rise of China and other nations has challenged that dominance. As the world becomes more interconnected, it is important for the United States to identify which technologies will be future geopolitical battlegrounds.

There are a number of factors that should be considered when making this determination. First, it is important to identify which technologies are critical to the United States’ economic and national security. These are the technologies that the United States must maintain a competitive edge in order to protect its interests.

Second, it is important to consider which technologies are becoming

14 SCSP generated this text with a LLM developed by [Anthropic](#). SCSP takes ultimate responsibility for the content of this publication.

15 SCSP generated this text with [Bloom-2b5](#), an LLM developed by Huggingface. SCSP takes ultimate responsibility for the content of this publication.

16 SCSP generated this text with a LLM developed by [Anthropic](#). SCSP takes ultimate responsibility for the content of this publication.

increasingly important globally. These are the technologies that other nations are investing in and developing, and which could give them a competitive advantage over the United States.

Finally, it is important to consider which technologies are emerging and have the potential to be game-changers. These are the technologies that could upend the status quo and create new opportunities for the United States. The United States must be proactive in identifying which technologies will be future geopolitical battlegrounds. By doing so, it can ensure that it remains a world leader in these critical areas.” — **GPT-3**¹⁷

As impressive as these responses may be, today’s state of the art LLMs still produce responses that are subject to bias, are irrelevant, and/or can present incorrect information as if it were factual. These models are also limited by the quality and recency of the data on which they are trained. For example, Anthropic’s model, trained on data from 2021, produced the following response:

What is the likelihood that Russia invades Ukraine in 2022?

“The likelihood that Russia will invade Ukraine in 2022 is low. Russia is unlikely to risk a major military confrontation with Ukraine and its allies by invading next year. Russia has shown little interest in resuming large-scale hostilities in Ukraine after the conflicts of 2014 and 2019. However, Russia could take other aggressive actions against Ukraine in 2022, such as conducting cyber attacks or military exercises near the border.” — **Anthropic**¹⁸

Most humans paying attention to the news would know that Russia invaded Ukraine in 2022 because our understanding of the world around us updates in real-time. However, an AI model trained on a static dataset from 2021 would not have knowledge of Russia’s invasion until retrained on new data. Nevertheless, the Anthropic model’s answer may in fact represent conventional wisdom at the time it was trained, failing, like many human analysts did at the time, to predict Russian President Vladimir Putin’s behavior.

LLMs reflect both the promise and perils posed by AI and emerging technologies writ large. While LLMs contain significant limitations today and will always carry associated risks, they are on pace to advance at an accelerating rate, with various research efforts underway around the globe to continue to advance the state of the art. As

¹⁷ SCSP generated this text with [GPT-3](#), an LLM developed by OpenAI. SCSP takes ultimate responsibility for the content of this publication.

¹⁸ SCSP generated this text with a LLM developed by [Anthropic](#). SCSP takes ultimate responsibility for the content of this publication.

these models become ever more capable, nations will undoubtedly seek to harness them for economic, military, and national security advantage. Governments will also be challenged to decide if and how these models should be regulated to ensure they are not employed for nefarious purposes. With China determined to surpass the United States in AI leadership, democracies must choose whether to shape and constrain these models in line with our values, or cede this cornerstone of the international competition to a rival.

Compute

Regarded as a mature GPT, computing remains a key driver of progress in AI, facilitated by continued progress in microelectronics. Today, the locus of compute is evolving.¹⁹ Edge computing could alter the roles of the data center and the cloud and drive new requirements for efficient processors and improved networking.²⁰ The nation needs continued investment to compete in promising novel computing paradigms. As existing semiconductor technology runs up against the laws of physics with the end of Moore's law,²¹ multiple paradigms appear to be on the cusp.

In *quantum computing*, the United States continues to demonstrate technical progress, bringing practical quantum computing closer to reality.²² Once successfully scaled, quantum computing will be important for national security and provide economic benefits by enabling simulations of complex phenomena that cannot be performed today.²³ Opportunities also exist for the United States to work with European and Japanese partners to ensure a secure supply chain of critical quantum computing components.²⁴ Meanwhile, advances in microelectronics, such as low-cost, extremely low-power transistors,²⁵ will make possible novel paradigms like *neuromorphic computing*, which models the human

¹⁹ John Shalf, [The Future of Computing Beyond Moore's Law](#), The Royal Society (2020).

²⁰ Haftay Gebreslasie Abreha, et al., [Federated Learning in Edge Computing: A Systematic Survey](#), Sensors (2022).

²¹ "Moore's Law is a techno-economic model that has enabled the information technology industry to double the performance and functionality of digital electronics roughly every 2 years within a fixed cost, power and area." John Shalf, [The Future of Computing Beyond Moore's Law](#), The Royal Society (2020).

²² Edward Parker, et al., [An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology](#), RAND Corporation (2022).

²³ NIST announced its selection of the first set of quantum resistant encryption algorithms in July 2022. Quantum computers hold the potential to be able to break the encryption standards widely in use today. NIST's selection is a key step towards transitioning to quantum resistant cryptographic algorithms. [NIST Announces First Four Quantum-Resistant Cryptographic Algorithms](#), National Institute of Standards and Technology (2022); [Quantum Computing Applications and Simulations](#), U.S. Department of Energy (last accessed 2022).

²⁴ Edward Parker, et al., [An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology](#), RAND Corporation (2022).

²⁵ Sungsik Lee & Arokia Nathan, [Subthreshold Schottky-Barrier Thin-Film Transistors With Ultralow Power and High Intrinsic Gain](#), Science (2016).

mind.²⁶ *Biological computers* — which use molecules such as proteins and DNA as inputs to cells — are also becoming increasingly feasible and could unlock an entirely new way to perform computational calculations and store and process data. For example, researchers in early 2022 demonstrated the feasibility of archiving images and videos in the DNA of living *E. coli* cells.²⁷

Networks

Building on the transformational impact of the information and communication technologies (ICTs) that digitized our world, the Internet of Things and next generation networks — and linkages with the physical and biotechnical worlds — will create wide-ranging impacts and remain an arena of competition.²⁸ China is increasingly also a key player in the building of undersea cables,²⁹ and is emerging as a competitive player in the digital platforms that the world uses for communicating and processing data.³⁰ The United States and its allies need to not only plug this existing gap but must also lean forward to develop future network technologies, which could include next generation wireless networks (i.e. 6G), satellite Internet constellations like Starlink, and other novel paradigms. One moonshot-like objective would be a *ubiquitous, secure global connectivity program* from a space-based constellation that would expand connectivity to the Internet for underserved areas within the United States while also providing a platform to help global populations circumvent censorship by authoritarian regimes.³¹

The competition to define 6G is already beginning.³² The United States will likely need to work closely with key partners and allies that host wireless equipment manufacturers to ensure that 6G is developed and available on the market with reasonable speed, to avoid domination by Chinese firms.³³ Meanwhile, advances in *quantum communications networks* that use quantum phenomena to control and transmit information could lead to the emergence of a highly secure “quantum internet” by the end of the decade.³⁴ The

26 David Rand, [What's This Neuromorphic Computing You're Talking About?](#), Hewlett Packard Enterprise (2021).

27 Emily Waltz, [Scientists Store Video Data in the DNA of Living Organisms](#), IEEE Spectrum (2017).

28 Volker Ziegler, [How to Make 6G the Next General Purpose Technology](#), IEEE (2021).

29 Matthew Goodman, [Securing Asia's Subsea Network: U.S. Interests and Strategic Options](#), Center for Strategic and International Studies (2022).

30 Zheping Huang, [TikTok Turns On the Money Machine](#), Bloomberg (2022); Alice Kantor, [Cloud Becomes New Front Line Between China and the West](#), Financial Times (2021).

31 SpaceX's Starlink program has already demonstrated the technical capacity for such systems. See Paulina Duran, [SpaceX's Starlink Expects It Can Provide Global Coverage Around September](#), Reuters (2021).

32 Michael Koziol, [6G is Years Away, but the Power Struggles Have Already Begun](#), IEEE Spectrum (2021).

33 [Trivium Tech Daily: June 22, 2022](#), Trivium China (2022).

34 Cade Metz, ["Quantum Internet" Inches Closer with Advance in Data Teleportation](#), The New York Times (2022).

Department of Energy’s 2020 blueprint could serve as the basis for a bold national effort to realize such a network.³⁵ China was the first country to send intertwined quantum particles from a satellite to ground stations in 2017,³⁶ and will likely continue to invest heavily in researching quantum communications networks.³⁷

Biotechnology

Synthetic biology will transform sectors as diverse as agriculture, materials, and energy.³⁸ Several factors are behind these advances: the coupling of biotechnology research with AI;³⁹ the decreasing costs in genomic sequencing (at a rate faster than Moore’s Law);⁴⁰ the improving capacity to rapidly synthesize DNA; and the advancing ability to manipulate biological systems to produce specific chemical and molecular compounds.⁴¹ The United States is today the global leader in genetic engineering and molecular biology,⁴² and has an opportunity to unleash an entire “bioeconomy”⁴³ that is estimated to eventually be worth anywhere between \$4-30 trillion and capable of producing up to 60 percent of the physical inputs to the global economy.⁴⁴ An example of a bold biotechnology objective would be to create a *national synthetic biology stack* – akin to an application programming interface (API) for software – that could enable more companies and researchers to expedite and scale the production of new products like materials in the short term and enable the engineering of more complex biological systems down the road. The United States also could scale DARPA’s Pandemic Prevention Platform (P3)⁴⁵ into a broader and true “BioShield” for the nation that combines specific technology aspects and public-

35 [U.S. Department of Energy Unveils Blueprint for the Quantum Internet at ‘Launch to the Future: Quantum Internet’ Event](#), U.S. Department of Energy (2020).

36 Gabriel Popkin, [China’s Quantum Satellite Achieves ‘Spooky Action’ at Record Distance](#), Science (2017).

37 Rachel Courtland, [China’s 2,000-km Quantum Link Is Almost Complete](#), IEEE Spectrum (2016); [The World’s First Integrated Quantum Communications Network](#), Phys.org (2021).

38 [2022 Trends Report: Synthetic Biology, Biotechnology, & AgTech](#), Future Today Institute (2022); Christopher A. Voigt, [Synthetic Biology 2020-2030: Six Commercially-Available Products That are Changing Our World](#), Nature Communications (2020).

39 See e.g., Neil Savage, [Tapping Into the Drug Discovery Potential of AI](#), Biopharma Dealmakers (2021).

40 Kris A. Wetterstrand, [DNA Sequencing Costs: Data](#), National Human Genome Research Institute (2021).

41 [Future Today Institute 2022 Tech Trends Report Synthetic Biology, Biotechnology, Agtech](#), Future Today Institute (2022).

42 [Task Force on Synthetic Biology and the Bioeconomy](#), Schmidt Futures (2022).

43 The Congress, through the National Defense Authorization Act for Fiscal Year 2022, created the National Security Commission on Emerging Biotechnology as a strong positive and initial step to harness biotechnology. Pub. L. 117-81, [National Defense Authorization Act for Fiscal Year 2022](#) (2021). This congressional action can be all the more impactful if complimented by development of a coordinated national-level action to generate a strategic vision, efforts to address talent development, and efforts to bolster the commercial ecosystem such as development of a distributed network of domestic biomanufacturing facilities around the country.

44 Michael Chui, et al., [The Bio Revolution: Innovations Transforming Economies, Societies, and Our Lives](#), McKinsey Global Institute (2020); [Remarks by NSC Senior Director for Technology and National Security Tarun Chhabra at the Brookings Institution](#), Brookings (2022) (at 19:19 minutes).

45 Amy Jenkins, [Pandemic Prevention Platform \(P3\)](#), Defense Advanced Research Projects Agency (last accessed 2022).

private partnerships to “shield” the nation against future biological disasters.

Energy Generation and Storage

Growing private sector investment and innovation in both nuclear fission and fusion electricity production offer an alternative pathway to meeting future U.S. — and global — energy needs and satisfy national security and climate goals.⁴⁶ Novel fission reactor designs presage smaller reactors that cost less to build and are safer to operate.⁴⁷ Significant progress in fusion machines capable of producing more energy than they consume indicates that practical fusion power generation may finally be within reach in the next decade.⁴⁸ Fusion energy offers a step change that could amount to a zero-carbon way of producing energy that upends the long-standing energy geopolitics, reducing reliance on foreign energy markets, and advancing a wide array of other fields, including some that we cannot yet predict. Nuclear energy is a priority for China, which is planning to spend \$440 billion to build 150 new reactors in the next 15 years, more than the rest of the world has built in the past three decades,⁴⁹ while concurrently researching fusion machines for energy generation.⁵⁰

A bold national objective would be to call for delivery of *fusion energy* to our national grid by 2028.⁵¹ A bar-setting challenge could incentivize a race among U.S. fusion developers to cross the breakeven threshold for a fusion machine — producing more energy than it consumes — could catalyze a world-leading fusion energy industry that addresses long-term national security and climate goals.⁵² The importance of national *energy storage* objectives will march together with demand for new sources of energy generation. Continued U.S. investment in the development of novel energy storage technologies — especially alternative chemistries beyond lithium-ion⁵³ — and domestic battery manufacturing

46 Lizette Chapman, [Tech Billionaires Rally Around Nuclear as Energy Crisis Looms](#), Bloomberg (2022).

47 Zach Winn, [Commercializing Next-Generation Nuclear Energy Technology](#), MIT News Office (2020).

48 [Helion Passes 100 Million Degrees Celsius](#), World Nuclear News (2021); David Chandler, [MIT-designed Project Achieves Major Advance Toward Fusion Energy](#), MIT News Office (2021); see also [Readout of the White House Summit on Developing a Bold Decadal Vision for Commercial Fusion Energy](#), The White House (2022).

49 Dan Murtaugh, [China's Climate Goals Hinge on \\$440 Billion Nuclear Buildout](#), Bloomberg (2022).

50 Ben Turner, [China's \\$1 Trillion 'Artificial Sun' Fusion Reactor Just Got Five Times Hotter than the Sun](#), Live Science (2022).

51 Multiple leading commercial companies now project that they will complete a successful demonstration of a net-positive fusion reaction within the next few years and plan to launch fully-operational facilities by 2030. See [The Global Fusion Industry in 2022](#), Fusion Industry Association (last accessed 2022). Additionally, the U.S. Government recently launched a laudable decadal vision for commercial fusion energy. [Readout of the White House Summit on Developing a Bold Decadal Vision for Commercial Fusion Energy](#), The White House (2022).

52 [60 Years of Progress](#), ITER (last accessed 2022).

53 Energy Report Part 1: Energy Storage, TechNext (2022) (*SCSP-commissioned work product*).

capability will only grow in strategic importance,⁵⁴ as improvements in batteries are likely to undergird progress in a host of future transportation technologies from electric and flying cars to delivery drones, as well as making a renewable energy-based grid a reality.⁵⁵ China's hold on today's battery supply chain underscores the importance of U.S. innovation and investment in this area to insulate itself from geopolitical risk.

Smart Manufacturing

The United States cannot match China's manufacturing dominance but it can offset it.⁵⁶ The emerging biomanufacturing sector, technologies such as AI, and additive manufacturing, present the United States new opportunities to build on existing efforts to revitalize and reinvent its manufacturing base.⁵⁷ A strong domestic manufacturing capability is also key to a vibrant innovation ecosystem as it reduces the barriers for bringing new technologies to market.⁵⁸ Biomanufacturing could serve as the basis of a future multi-trillion dollar manufacturing base and provides another opportunity for the United States to regain a foothold in industries that have migrated to other locales.⁵⁹ The combination of *AI, augmented/virtual reality, additive manufacturing, and robotics* can be harnessed for manufacturing to enhance productivity and quality, improve worker training, and allow factories to more quickly reorganize themselves to change what they produce on demand.⁶⁰ The creation of digital twins coupled with AI-based simulation and modeling can also reduce costs and optimize production processes.⁶¹ New models for deploying robotics where small firms are able to acquire robots-as-a-service could also enable more U.S. manufacturers to take advantage of the productivity gains provided by automation.⁶²

Opportunities and Threats

Technology holds amazing potential to solve some of the greatest challenges of our time.

54 [Final Report](#), National Security Commission on Artificial Intelligence at 265-266 (2021).

55 Joann Muller, [Flying Taxis, Delivery Drones and More are Finally Taking Off](#), Axios (2022).

56 Felix Richter, [China Is The World's Manufacturing Superpower](#), Statista (2021).

57 SCSP engagement with a venture capital firm (April 2022); [The Biden-Harris Plan to Revitalize American Manufacturing and Secure Critical Supply Chains in 2022](#), The White House (2022); John F. Sargent Jr., [The Obama Administration's Proposal to Establish a National Network for Manufacturing Innovation](#), Congressional Research Service (2014).

58 Katie Rae, [2021 Tough Tech Landscape](#), The Engine (2021).

59 Michael Chui, et al., [The Bio Revolution: Innovations Transforming Economies, Societies, and Our Lives](#), McKinsey Global Institute (2020). The White House has a plan to "revitalize American manufacturing and secure critical supply chains," although the plan does not mention biomanufacturing specifically. See [The Biden-Harris Plan to Revitalize American Manufacturing and Secure Critical Supply Chains in 2022](#), The White House (2022).

60 See J.S. Srari, et al., [Unlocking Business Model Innovation Through Advanced Manufacturing](#), World Economic Forum at 18-19 (2022).

61 Scott Martin, [What Is a Digital Twin?](#), Nvidia (2021).

62 Thomas Black, [Robot Subscription Services Let Companies Automate on the Cheap](#), Bloomberg (2022).

Yet it can also produce novel threats. Harnessing the opportunities while neutralizing the threats will require concerted national efforts. Could *water technology* address fundamental issues like the availability of water for the human race? Water scarcity is increasingly a global challenge with national security implications for the United States.⁶³ Yet investment in technological innovations to meet these challenges remains limited and breakthroughs have lagged as a result.⁶⁴ What about *neutralizing AI-enabled disinformation platforms* that use autonomy to divide our nation? While many existing efforts aim to detect and remove mis- and disinformation,⁶⁵ concerted efforts across government, the private sector, and philanthropy could focus on improving citizenry resilience to mis- and disinformation. The appropriate toolset could include a suite of technologies alongside other types of interventions, such as improving education and media literacy.

As the world enters another disruptive technological age, the United States faces a rival in China that is already pivoting and positioning to dominate a similar slate of “deep tech” and “frontier tech.”⁶⁶ Whether the United States can rise to the occasion and harness the promise of the pending wave of revolutionary technologies will determine who wins the 21st century.

63 [U.S. Action Plan on Global Water Security](#), U.S. Department of State (2022).

64 A bold “water technology” goal such as scaling atmospheric water harvesting in projects like Hydration to Everyone (H2E) could yield significant global and national security benefits with a government nudge. [Harvesting Water from the Air](#), X (2021).

65 A sample of ongoing initiatives in both government and the private sector includes the Department of State’s [Global Engagement Center](#), the FBI’s [Foreign Influence Task Force](#), the [Election Integrity Partnership](#), the Atlantic Council’s [Digital Forensic Research Lab](#), the Poynter Institute’s [International Fact-Checking Network](#), and various Internet platforms’ content moderation efforts.

66 Kimberly Cairns, [Why China is on its Way to be World’s Next Leader of Deep Technology](#), *The West Australian* (2022); [What Tech Does China Want?](#), *The Economist* (2021); Arjun Kharpal, [In Battle with U.S., China to Focus on 7 ‘Frontier’ Technologies from Chips to Brain-Computer Fusion](#), *CNBC* (2021).

Appendix: Contribution List

Mid-Decade Challenges to National Competitiveness



Appendix: Contribution List

Chair

Dr. Eric Schmidt

CEO

Ylli Bajraktari

Board of Advisors

Michèle Flournoy

Robert O. Work

Dr. Nadia Schadlow

William “Mac” Thornberry III

SCSP Staff

Executive Staff

Michael Gable

Angela Ponmakha

Integration Team

Ylber Bajraktari

Chelsea Holt

Seth Center

PJ Maykish

Public Affairs, Government Affairs, Legal, and Operations Teams

Sarah Johnson

Ariana Orne

Jennifer Sheehan

Mike Lueptow

Rachel Pankuch

Jamie Tomberlin

Brandon McKee

Tara Rigler

Panel Teams

Jafer Ahmad

Abigail Kukura

Rob Nelson

Tooba Awan

Katherine Kurata

Katie Stolarczyk

Ben Bain

David Lin

Rick Switzer

Rama Elluru

Justin Lynch

Liza Tobin

Jefferson Gee

Peter Mattis

Luke Vannurden

Hina Gir

Will Moreland

Meaghan Waff

Brady Helwig

Emma Morrison

Joe Wang

Chuck Howell

Lauren Naniche

Warren Wilson

Research Assistants

Caroline Agsten	Daniel Freedline	Evan Miller
Ricky Altieri	Emma Gallagher	Fiona Pollack
Sophie Baine	Anabel Heisley	Cole Rubin
Karina Barao	Humza Jilani	Louis Santoro
Jessica Burrell	Abhinav Kumar	Nyah Stewart
Shaantam Chawla	Sabrina Laub	Kimberly Syuardi
Ryan Chen	Christie Lawrence	Itallya Taylor
Stephen Coles	Channing Lee	Tetiana Tsunik
Annabelle Darby	Sofia McGettigan	Aristotle Vainikos
Asher Ellis	Eamon McKeever	

From October 2021 until August 2022, SCSP organized 4 board meetings and 26 panel meetings that included more than 225 experts, government officials, academic leaders, and many others. The SCSP staff also conducted more than 400 engagements with leaders from the private sector, academia, civil society, and government. We are grateful for the time and effort of those we have consulted. This report is the culmination of the SCSP staff's work up to this point in its mandate and its effort to synthesize the wealth of information gathered from all of the individuals and entities with whom we have engaged. Although not everyone we have engaged with may endorse this report, we hope it reflects the key points we have learned and charts a path for action.

SCSP and Panel Advisors

Christopher Ahlberg	Bonnie Glick	DJ Nordquist
Robert D. Atkinson	Greg Grant	Matt Pottinger
Nick Beim	José-Marie Griffiths	John Raidt
Hal Brands	Reid Hoffman	Condoleezza Rice
Erik Brynjolfsson	Ben Horowitz	Steve Rosen
Mignon Clyburn	Eric Horvitz	Jonathan Rosenberg
David Danks	Amy Jan	Raj Shah
Chris Darby	Chris Kirchoff	Jack Shanahan
Rodney Faraon	Kevin McGinnis	Dean Souleles
Nate Fick	Michael McQuade	Alex Younger
Christine Fox	Dawn Meyerriecks	Amy Zegart
Glenn Gaffney	Mark Montgomery	
Michael Garris	Gina Neff	

We also say a special thanks to the following individuals for supporting our work and without whom this report would not have been possible.

David Agranovich	Erik Britton	Jeff Ding
Younghoon Ahn	Emerson Brooking	Gerard DiPippo
Nathaniel Ahrens	Mike Brown	Dante Disparte
Michael Allen	Peter Brown	Jessica Drun
Bastian Alm	William Burruss	Ian Dsouza
Slavina Ancheva	Scott Carpenter	Allison Duettmann
Megan Anderson	James Cerven	Regina Dugan
Gary Ang	Ting Chang	David Edelman
Taka Ariga	Rebecca Chapman	Tyler Ellis
Sunami Atsushi	Victoria Chernow	Alex Engler
Azeem Azhar	Matt Chessen	Kata Escott
Omer Bab	Rumman Chowdhury	Stephen Ezell
Dan Babich	Eric Chua	Rebecca Fair
Justin Bassi	Bryan Clark	Pat Falcone
Jon Bateman	Jack Clark	Ryan Farris
Kathy Baxter	Cathryn Clüver Ashbrook	Peter Fatelnig
David Beaumont	Harry Coker	David Feith
Alexandra Belias	August Cole	Steven Feldstein
Olga Belogolova	Anthony Corso	Joe Felter
Paul Benfield	Thomas Creely	Sim Feng-Ji
Brando Benifei	Ian Crone	Leah Fiddler
Nicholas Berliner	Audrey Kurth Cronin	Frank Finelli
Erik Bethel	Daniel Crosby	Aria Finger
Meghan Biery	Tino Cuellar	Edward Fishman
Vladimír Bilcík	Christine Custis	Benedikt Franke
Steve Blank	Mette Vestergaard Dam	Aaron Friedberg
Richard Boly	Joanna Davies	Julia Friedlander
Katherine Boyle	Emily de la Bruyère	Adam Frost
Nick Bramble	Tess Deblanc-Knowles	Cherif Gamra
Jessica Brandt	Loren DeJonge Schulman	Jennifer Ganten
Timo Bremer	Ana De Sousa	Avichal Garg
Andrew Brigden	Nathan Diller	Diana Gehlhaus

Mircea Geoana	Jason Hsu	Dave Kriete
Sennay Ghebreab	Robin Hu	Matt Kroenig
Erwin Gianchandani	Cordell Hull	Thomas Krueger
David Gitter	Michael Hunzeker	John Krumm
Raphaël Glucksmann	Andrei Iancu	Ashish Kumar
Logan Graham	Marco Iansiti	Lynn Kuok
Josh Griffiths	Mounir Ibrahim	Scott Lacy
Sophie Guelff	Elnigar Iltebir	Farhaan Ladhani
Abhishek Gupta	George Ingram	Megan Lamberth
Ilan Gur	Nathalie Jaarsma	Timea Lapsanszki
Natalie Gutman-Chen	Jonathan Jackson	Han Yang Lau
Meeri Haataja	Rose Jackson	Travis Leblanc
Ryan Hagemann	Jahn Jeffrey	Naomi Lefkovitz
Erin Hahn	Amy Jenkins	Claire Leibowicz
Stephanie Hall	Andrew Jenks	Paul Lekas
Marin Halper	Bruce Jentleseon	Bernard Leong
Sarah Hamburg	Suin Jeong	Eric Levesque
T.X. Hammes	Matthew Johnson	Greg Levesque
David Hanke	Chris Jones	Stuart Levey
William Hannas	Frederick Kagan	Erik Limpaecher
Emily Harding	Kimberly Kagan	Kevin Loane
Kerri Haresign	Eva Kaili	Douglas London
Andrew Harris	Ivan Kanapathy	Gene Loughran
Todd Harrison	Rob Katz	Tammy Ma
Alexander Harstrick	Dan Kaufman	Christopher Magee
Jake Helberg	Bilahari Kausikan	Joshua Marcuse
Jon Hillman	Sugie Kazuhiro	Dana Marshall
Suzuki Hiromasa	Michael Kearney	Svetlana Matt
Peter Ho	Jaclyn Kerr	Eva Maydell
Frank Hoffman	Emily Kilcrease	Alexandra McCarroll
Joan Hoffman	Jan Kleinnijenhuis	Andrew McCosh
Orin Hoffman	Alexander Kott	Georgia McKenna
Samantha Hoffman	Pete Kouretsos	Milo Medin
John Holdren	Saiki Kozo	James Meeks
Mat Honan	Adam Kozy	Sultan Meghji
David Hoyt	Sarah Kreps	Walker Mills

James Mismash	Mackenzie Rice	Joshua Stiefel
Jim Mitre	Heather Jo Richman	David Stilwell
Evan Miyazono	Gary Rieschel	Jeff Stoff
Nand Mulchandani	Margaret Roberts	David Stout
James Mulvenon	Mikel Rodriguez	Rob Strayer
Ben Murphy	Andrew Rollo	Karen Sutter
Richard Murray	Dan Rosen	Walter Sweet
Jeffrey “Jeb” Nadaner	Mark Rosenblatt	Ikawa Takahiro
Anu Narayanan	Anshu Roy	Adam Thierer
Dan-Flaviu Nechita	Mindy Rudell	Drew Thompson
Richard Nephew	Mick Ryan	John Thornill
Antti Niemela	David Sandson	Tomicah Tillemann
Nazak Nikakhtar	Chad Sbragia	Andrew Tilton
Martijn Nuijten	Geoff Schaefer	Simon Thorup Trier
Kevin O’Connell	Kendra Schaefer	Kathy Trimble
Enrique Oti	Bill Scherlis	Christian Trotti
Marc-Etienne Ouimette	Chris Schroeder	Dragos Tudorache
Nina Palmer	Brian Scott	Zachery Tyson Brown
Andy Parsons	Mark Seip	Sander van der Linden
Mark Pascale	Michael Sellitto	Michel van Leeuwen
Cheri Pascoe	Neil Serebryany	David van Weel
Alka Patel	Pratik Shah	Hal Varian
Terry Pattar	Wade Shen	Brett Vaughan
Carolyn Patteson	Justin Sherman	Michael Vickers
Kenneth Payne	Reshma Shetty	Karin von Hippel
Jon Pelson	Matt Shortal	Rick Waddell
Carlota Perez	Yachi Shotaro	Meredith Wallace
Jason Pielemeier	Rebecca Shrimpton	Jacob Wallis
Anna Puglisi	Anuraag Singh	Tim Walton
Katie Rae	Pavneet Singh	Alex Wang
Maithra Raghu	Peter Slort	Jonathan Ward
Devaki Raj	Larry Smith	Becca Wasser
Jai Ramaswamy	Brian Spears	Emily S. Weinstein
Eric Redmond	Dan Spokojny	Joe White
Will Regan	Danica Starks	Gavin Wilde
Rob Reich	Ian Stewart	Sean Williams

John Mark Wilson
Edward Wittenstein
Kevin Wolf
Anna Wong
Marcel Worrying

Jeff Wu
Kevin Xu
Tadao Yanase
Jessica Young
Qasar Younis

Zaid Zaid
Justin Zeefe
Cobun Zweifel-Keegan
John Zysman

A special thanks to Lirijon Kadriu for designing the SCSP logo.



SPECIAL COMPETITIVE
STUDIES PROJECT

