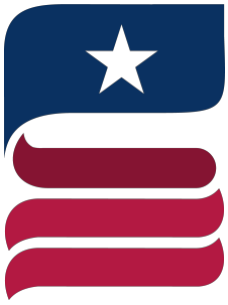
NATIONAL ACTION PLAN FOR U.S. LEADERSHIP IN

Advanced Networks

SPECIAL COMPETITIVE STUDIES PROJECT



The Special Competitive Studies Project (SCSP) is a bipartisan, non-profit project with a clear mission: to make recommendations to strengthen America's long-term competitiveness where artificial intelligence (AI) and other emerging technologies are reshaping our national security, economy, and society.

Authors

Warren Wilson
Director for Economy

Liza Tobin
Senior Director for Economy

PJ Maykish
Senior Advisor

David Lin
Senior Director for Platforms

Joe Wang
Senior Director for Foreign Policy

Tooba Awan
Director for Economy

Katie Stolarczyk
Associate Director for Economy

Brady Helwig
Associate Director for Economy

Contributors

This report benefited greatly from insights and expertise by a number of individuals to whom we are deeply grateful. It aims to reflect many, though not all, of those insights.

Robert D. Atkinson
Scott Kelly
Paul Mankiewich
Amit Mital
Milo Medin
Tommaso Melodia
DJ Nordquist
Jon Pelson
John Raidt
Nadia Schadlow
Tom Power
Robert E. Wheeler

A Letter from the Chairman & the CEO

SCSP is developing a series of National Action Plans to establish U.S. leadership in key technology areas. This action plan addresses advanced network technology, which will transform industries as diverse as agriculture, manufacturing, logistics, and education, merging virtual and physical reality in ways that today we can only begin to foresee. The development of networks and artificial intelligence (AI) will be increasingly intertwined as AI plays an expanding role in managing and animating networks, and networks embedded with more sensing and computing power will channel vastly more data into training AI models.

It is critical that the United States, along with its allies and partners, maintain global leadership in advanced network technologies given the national security implications. We are entering an era that presents considerable risks and immense opportunities to transform our world by revolutionizing how we connect via next-generation, digital pathways that also animate autonomous vehicles, robotics, and smart communities.

While U.S. innovators led development and commercialization of modern network technology, China has taken the lead in producing and exporting telecommunications equipment and building networks, particularly fifth-generation (5G) mobile networks technology. Yet the race is just beginning to harness 5G and advanced network technologies for next-generation industrial and security applications. Reasserting U.S. leadership in this sector requires not only rebuilding network supply chains, but also doubling down in segments where America remains competitive, including fiber optic and subsea cables, satellite communications, and cloud computing, as well as in emerging technologies such as free space optical networks (FSONs).

U.S. leadership in producing and exporting network technologies would promote democratic values and data security norms in cyberspace globally. We must take action. Winning this competition will require sustained focus by the government, greater public-private collaboration, and a willingness to make strategic bets on network technology, high-value applications, and solutions for providing trusted network technology around the world. Drawing on expertise from the private sector, academia, and government, this advanced networks action plan combines bold technology "moonshots" with recommended changes to the innovation ecosystem along with policies to position the U.S. for durable advantage.

Rather than address every aspect of this vast sector, SCSP's action plan focuses on solving for U.S. advantage from a national security perspective. We invite you to join us in this effort to ensure that America is positioned and organized to win the techno-economic competition between now and 2030, the critical window for shaping the future.

Eric Schmidt,
Chairman, SCSP

Ylli Bajraktari,
President & CEO, SCSP

Introduction

Advanced wired and wireless networks form the backbone of the digital economy and the modern world. These networks not only underpin global communications, but are increasingly embedded with computing, sensing, and artificial intelligence (AI) capabilities fusing the digital and physical worlds and bringing to life autonomy, robotics, and metaverse uses. Nations that lead in the development and production of advanced network hardware and software will control the sea lanes of cyberspace and enjoy first-mover advantages in network-enabled applications. While the United States was long a world leader in network technology, industry mismanagement and policy neglect allowed its telecommunications equipment producers to falter in recent decades as the People's Republic of China (PRC) took a commanding lead in building the world's connectivity infrastructure, including fifth-generation (5G) wireless networks. Yet the race is just beginning to develop 5G and advanced network applications, like smart manufacturing and smart cities, that can drive future economic growth and security.[1]

Action is needed to better position the United States to lead "the next 5G" of foundational network technology. The United States lacks major producers of end-to-end telecom solutions for domestic networks and export, and has no national-level strategy to harness networks to achieve the nation's economic, social, and national security aspirations. The U.S. radio spectrum pipeline for mobile networks remains stalled, even as bipartisan leaders publicly tout the strategic importance of 5G and 6G. Yet the United States still has powerful tools with which to reassert global advantage in advanced networks. These include international leadership in cloud, software, and space technologies, which are increasingly integrated into telecom networks, as well as a world-class, diverse innovation ecosystem.

U.S. leadership in such a critical general purpose technology cannot be left to chance. SCSP developed this national technology action plan to provide an advanced networks policy roadmap for a coordinated effort among the private sector, academia, and government to establish U.S. leadership in this critical technology through 2030, alongside our allies and partners. U.S. leaders must think beyond the recent policy focus on 5G networks to encompass other elements of the connectivity stack, including low-earth orbit (LEO) satellites, data centers, and potential leapfrog technologies, like free space optical communications and networks (FSONs).

Desired Endstate

By 2030, the United States will have **secure**, **cutting-edge networks throughout the country** that facilitate pervasive connectivity and productive network applications (such as smart cities and ports, autonomy, robotics, and other use cases) for inclusive economic and social benefit, as well as competitiveness in global markets..

By 2030, the United States and its allies and partners:

- **Lead development of new network technology and production of advanced network hardware** in a competitive ecosystem that is not dependent on China and other adversary nations;

- **Export complete, cost-effective digital infrastructure packages** to developing and emerging economies; and

- Ensure that international technology standards for 6G wireless and other network technology **support the open internet, free flow of information, personal data privacy, and other democratic objectives.**

Central Goal

Reassert U.S. leadership in telecommunications technology development and production to expand secure, cutting-edge digital networks domestically and abroad by strategically investing in critical research and real-world technology pilots, and enacting policies that lower barriers to innovators and foster distributed, disruptive network innovation.

Action Plan Overview

Background

U.S. firms and institutional research produced much of the foundational technology for modern wireline and cellular networks. Yet, the United States and its allies now depend on a handful of non-U.S. firms for telecom networks.[2] The PRC recognized the strategic value of network technology and built world-leading telecommunications equipment producers through a "brute force economics"[3] approach of industrial policy and forced technology transfer. This approach, alongside U.S. government missteps and industry mismanagement, led to the demise of major North American telecom hardware producers — and gave the PRC a lead in the production and deployment of 5G wireless networks.[4]

Today, Huawei and ZTE hold roughly a 40 percent share of the $100 billion global telecommunications equipment manufacturing market – with Huawei leading all firms – compared to around 16 percent by U.S. producers.[5] China's leaders have leveraged increased network technology competitiveness to gain more influence in international standards setting bodies. U.S. government measures — such as adding Huawei to the Entity List[6], expanding the foreign direct product rule (FDPR)[7] and other restrictions on select ZTE equipment,[8] and a diplomatic campaign warning of the risk of digital dependence on the PRC[9] — have slowed but not stopped Huawei's 5G march. Policymakers have taken steps to address the the security risks, including import and installation prohibitions and mandating removal of components,[10] but U.S. authorities and firms are struggling to fund and execute these efforts.[11]

Government and industry stakeholders are promoting Open Radio Access Network (Open RAN) technology to reduce costs and increase vendor diversity and interoperability for wireless networks. In 2022, Congress appropriated $1.5 billion for Open RAN research and development through the Public Wireless Supply Chain Innovation Fund.[12] Though promising, these efforts must address novel security, integration, and commercialization challenges that the PRC is well-positioned to exploit.[13] Meanwhile, America's workforce has been losing the skills needed to reshore production of critical network components. These complex supply chain and production challenges require a concerted, well-funded effort that blends private sector dynamism and capital with a compelling national strategic vision and action plan.

The cautionary tale of 5G hardware serves as a reminder that, in the context of today's international competition, leadership in strategic technologies cannot always be left solely to the market. Enterprise-scale 5G applications have seen limited uptake in both the United States or China, although China has a national strategy to develop them.[14] China is also pressing for global market share in satellite[15] and cloud technologies that are increasingly integrated with cellular networks and could serve as the basis of future network paradigms to support commercial and military ambitions.[16]

Finally, a disconnect remains between the United States and its allies concerning the urgency of securing networks from PRC hardware-based risks.[17] Commercial competition among allies is beneficial but at times threatens to overshadow collaboration to ensure democratic leadership in next-generation 6G networks. The United States and its allies must harmonize their supply chain and standards planning more closely to protect the democratic, decentralized, and open nature of the global internet.

First Principles

The following first principles frame the national security and economic theory of the case for strengthening U.S. leadership in advanced networks:

- **Advanced networks comprise the backbone of the digital world and are vital for U.S. national advantage, security, and economic prosperity.**
- **Cutting-edge network technologies are only as effective as they can be broadly distributed and secured.**
- **The United States should accelerate adoption of high-value 5G applications while also leading development of 6G and other next-generation networks.**
- **Next-generation networks are driving increasing convergence between the physical and digital worlds, making security and privacy considerations even more important.**
- **Hardware components of networks make supply chain security a paramount concern.**
- **Winning the standards battle in advanced networks is vital to ensuring leadership by the United States and its allies and partners and countering Beijing's digital authoritarianism.**
- **Advanced network policies and innovations should be designed to help Americans see technology more as an enabler rather than a threat or barrier.**

ACTION PLAN RECOMMENDATION | 1 / 4

Innovate: Potential Moonshots for Advanced Networks

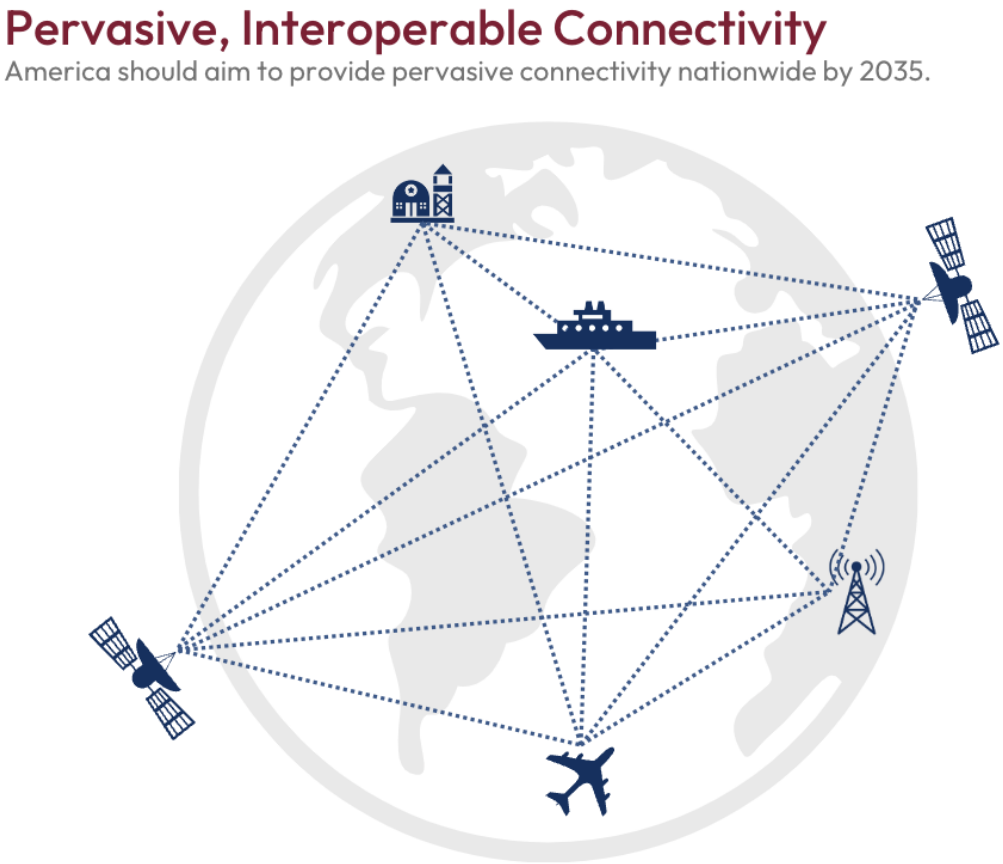
Moonshots are audacious goals that can move the entire U.S. innovation ecosystem toward a position of competitive advantage. These proposed goals are difficult, but they are attainable through a whole-of-ecosystem unity of effort like that of the Apollo program, which stretched America's sense of what was possible at the time it was conceived. The nation should create conditions to incubate new network paradigms and "moonshot" technologies that could render current commercial models and supply chain, spectrum, or other bottlenecks obsolete.

1.1 Pervasive, Interoperable Connectivity

Objective: The United States should aim to provide pervasive connectivity nationwide by 2035, with basic infrastructure in place by 2030. Pervasive connectivity would foster smart community and smart industry environments by integrating multiple, interoperable wired and wireless networks to support best-in-class autonomy, robotics, logistics, public safety, healthcare, and virtual reality.

Method: The U.S. government should set pervasive connectivity as the ultimate goal of current infrastructure buildouts and connectivity policies as part of a "National Digital Infrastructure Strategy," developed by the Federal Communications Commission (FCC) in conjunction with the Departments of Commerce, Homeland Security, Defense, and other relevant agencies. This strategy should extend beyond just addressing household broadband and also guide planning for both commercial and public sector enterprise connectivity needs. Beyond current broadband funding, federal and state governments must also continue to invest in connectivity

infrastructure. U.S. research agencies should work with firms to develop open application program interfaces (APIs) to support interoperability across all network nodes, including satellites, drones, ships, base stations, and devices. U.S. agencies should boost support and funding for research and development of AI technologies for network management and interoperability to unlock tremendous network efficiency and performance gains.



1.2 Global Leadership in Free Space Optical Communication and Networks (FSONs)

Objective: The nation should lead development of FSONs — which have the potential to revolutionize space communication — and scale the technology terrestrially as a new primary or supplementary connectivity option, particularly for secure communications.[18]

Method: The U.S. government should launch a national program to develop free space optical networks and communications as a mainstream connectivity means for terrestrial uses in security, industrial, logistics, agricultural, and household connectivity. The Space Development Agency[19] and DARPA's Space-BACN program is collaborating with commercial firms to scale these technologies among low-earth orbit (LEO) satellites, but its broader utility and commercial viability must be proven.[20] U.S. telecom supply chain security initiatives should incentivize U.S. and

allied sourcing and leadership of FSON components, building and testing more optical ground stations.

1.3 Building an Open Network Ecosystem

Objective: The U.S. government should accelerate adoption of open, interoperable public and private networks to facilitate innovation and a more secure supply chain.

Method: New technology — particularly Open RAN — allows entry points for new vendors and the opportunity to incubate a network equipment production and integration ecosystem. Rather than creating a national or state-owned telecom from scratch, the U.S. government should use grants and other incentives to new and existing technology and telecom firms to develop interoperable network solutions. The Public Wireless Supply Chain Innovation Fund has already appropriated $1.5 billion to support open network development, which should support real-world testing and development of high-consequence use cases.[21] U.S. authorities should also improve the policy environment for Open RAN by supporting interoperability certification and making more spectrum available (see section 3).

1.4 Win the 6G Race

Objective: The United States should pursue global leadership in producing inputs for building, and applying 6G networks by driving development of open network technologies, supporting real-world pilots for high-value use cases, and providing researchers with testbeds and spectrum.

Method: 6G is expected to build on the Internet of Everything and virtual reality use cases of 5G, which will be crucial to military and economic security. International 6G mobile network standard-setting is expected to begin in 2025, with commercial 6G network rollouts expected by 2030.[22] The United States has an historic opportunity to regain global leadership in mobile networks — but only with a clear U.S. government 6G strategy, serious research financing, and incentives for U.S. firms to make productive investments in network technology. This must be coupled with a concerted campaign to coordinate with like-minded foreign governments to shape international 6G standards (see section 4).

ACTION PLAN RECOMMENDATION 2 / 4

Build a Secure, Resilient Network and Supply Chain

Even the best "moonshot" technology requires sustainable commercial models to foster reliable supply and healthy competition. Over-reliance on a single supply source for critical infrastructure is risky.[23] It is even more problematic when that source is governed by an adversarial authoritarian regime with a demonstrated willingness and capability to weaponize its economic power for political reasons and export an autocratic model of technology governance.[24] The 5G/wireless landscape is also shifting with the integration of non-terrestrial networks (NTNs) transmitted via satellites and drones, expanding the critical infrastructure involved in these networks. U.S. government and private sector stakeholders should develop new network supply chains free of wireless core and RAN components produced in China and other adversary countries — or by PRC-owned vendors. They should do this through a combination of onshoring production, friendshoring[25] — using sources in allied and like-minded countries — and ensuring that the transition to open network architectures addresses new security vulnerabilities from the start.[26]

2.1 Catalyze New Production

Objective: The U.S. government should catalyze domestic and friendshored production of key network core, RAN, Internet of Things (IoT), and satellite components (antennae, radios, sensors etc.) through R&D funding, incentives, and further restrictions on PRC-made components.[27]

Method: Similar to recent incentives to spur semiconductor and battery production, Congress and Commerce should identify and enact stronger incentives for research, development, and

production of priority networking components. The $65 billion in Infrastructure Investment Act funding for broadband expansion[28] should also be used to purchase and incentivize secure supply chains for network components. Yet rather than implementing sweeping "Buy America" policies for U.S. government-funded broadband and network components,[29] U.S. officials should target a few priority components and offer favorable lending and incentives to firms able to scale production of those components domestically.

2.2 Create a Trusted Market

Objective: Use government procurement to create stable, consistent markets for trusted wireless components and large network deployments.

Method: The Department of Defense is already deploying enterprise-scale 5G networks on military installations for logistics and other use cases, with $600 million in funding to do so.[30] The U.S. government should deploy test networks in other environments, ranging from national parks to U.S. embassies, creating market demand for trusted vendors.

2.3 Fully Fund, Update, and Execute the Rip and Replace Program Managed by the FCC to Remove Designated, PRC-Origin Components[31] from U.S. Networks

Objective: Fully support U.S. network operators to complete replacement of untrusted components from U.S. networks.

Method: The FCC has concluded that the program's initial $1.9 billion in funding is insufficient by $3.7 billion,[32] a shortfall Congress must fill. Further delays will risk network failures, but mandating removal of PRC-origin equipment without sufficient government funding will leave U.S. carriers in a weaker financial position and even less able to invest in new, innovative infrastructure. Furthermore, failure to fund and implement this policy also undercuts U.S. attempts to persuade allies and partners to move away from Huawei and ZTE components.

2.4 Scale Open RAN Interoperability and Certification

Objective: Create standards and identify labs to verify interoperability and security of components and software applications with an open network paradigm, including IoT devices.

Method: The National Institute of Standards and Technology (NIST), the FCC, and other relevant agencies should scale efforts to create certification and interoperability standards for open network components, a crucial need for integrating components from different vendors. NIST and National Telecommunications and Information Administration (NTIA) should also direct research funding to developing the open-source "middleware"[33] software solutions for telecom networks to facilitate quicker, cheaper interoperability and ensure Open RAN introduces a competitive market. By building these solutions first and encouraging their commercial adoption, the United States can help shape the development of open network solutions globally.

2.5 Form a Public-Private Open Network Policy Group

Objective: Regularly convene key public and private sector stakeholders to solve execution and commercialization challenges.

Method: An independent, U.S.-based policy or technically focused organization(s) could regularly facilitate meetings of stakeholders in the U.S. market to discuss open network implementation and policy needs. This group can help develop a longer-term networks and digital infrastructure strategy for the United States.

2.6 Hardware Bill of Materials for Network Supply Chain Transparency

Objective: U.S. policymakers should introduce greater transparency into the network supply chain, helping incentivize trusted vendors.

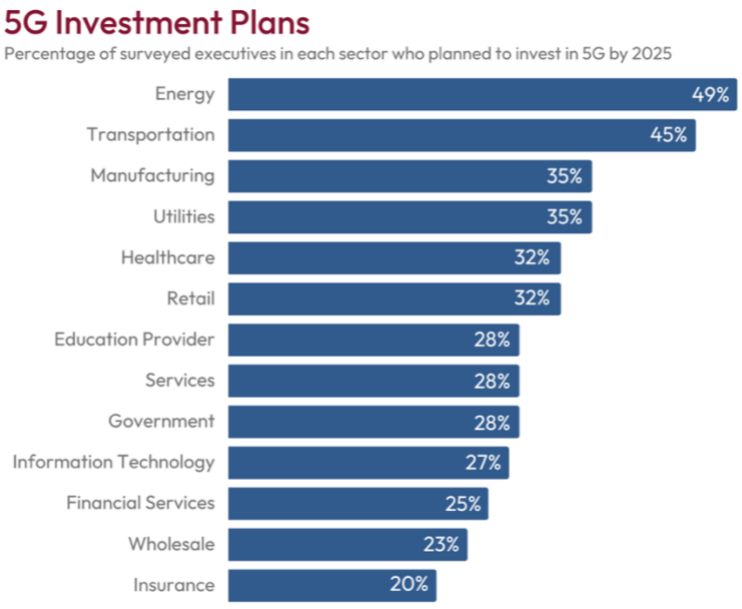
Method: NIST should require federal contractors to increase supply chain transparency by disclosing a hardware bill of materials for network components — and help incentivize procurement of secure components from transparent producers. A software bill of materials (SBOM) discloses all open source and third-party components present in a software application, and the Biden Administration recently issued a requirement for federal contractors to disclose an SBOM.[34] Through an Executive Order or Congressional action, U.S. policymakers could require a hardware bill of materials (HBOM) for federal contractors including detailed information on security validations, design intent, and country of origin for high-risk hardware.[35]

ACTION PLAN RECOMMENDATION | 3 / 4

Network Applications for Economic and Social Benefit

Imagine waking up in the year 2032. As you leave for work, your local Smart City hub monitors and redirects traffic flow, cutting your morning commute in half. An AI-enabled energy grid reduces carbon emissions and your energy bill by monitoring energy usage via billions of cloud-connected sensors and automatically redirecting power from a diversified array of energy sources including fusion energy. Smart factories around the country employ well-paid workers, aided by robots, to produce American-made goods on demand. Amidst all these devices, you are protected by commonsense data privacy laws, security practices, and privacy-protecting technology.

Much of the $13.2 trillion in the forecasted global value creation of 5G networks by 2035[36] lies in enterprise and city-scale network applications, which 6G networks would further advance. These range from industrial robotics to autonomous trucks fundamental to both economic competitiveness and military superiority. Up to 78 percent of enterprises recently surveyed across industries are investing in (or plan to invest in) 5G for business applications by 2025.[37] Sectors ripe for 5G private network innovation partnerships include healthcare, manufacturing, and logistics, including as part of smart city networks. The ability to configure and deploy private, enterprise-scale 5G networks could play to U.S. strengths in decentralized innovation, if the government takes steps to accelerate their testing, commercial viability, and adoption. Developing sustainable, profitable business models for 5G and beyond is also critical for continued private sector investment in next-generation networks, since mobile operators have thus far struggled to monetize 5G.[38] The U.S. government should accelerate and increase funding and partnerships for R&D of enterprise-scale, private 5G applications and smart city technologies. Chart Source[39]



3.1 "Warp Speed" for Networked Applications

Objective: Incentivize and promote the development of large-scale, commercializable network applications in priority sectors.

Method: NTIA, FCC, and sector-specific agencies should create challenge grants for the high-value networked applications coupled with a high-level public-private steering committee.[40] This program and funding should move beyond small grants currently available for technical advances[41] to incentivize large-scale applications in priority sectors such as advanced manufacturing, logistics, agriculture, and autonomy with clear commercial and security applications.

3.2 National Advanced Networks Incubators

Objective: American policymakers should elevate and expand the U.S. network of public-private 5G/6G testbeds launched through the Platforms for Advanced Wireless Research.[42]

Method: Federal funding for existing 5G innovation zones testbeds should be doubled from $50 to $100 million, with increased private sector funds, to support more startups and technology firms to test and develop commercializable industrial, autonomy, and security applications.

3.3. Autonomy Cities

Objective: Support real-world, integrated, city-scale autonomy testing.

Method: Autonomy applications are potentially the most consequential applications of advanced networks for security and prosperity. Safety, privacy, and cost concerns, however, make it difficult to test their use cases in the physical world at scale. The federal government, in partnership with U.S. firms, could provide significant grants and digital infrastructure upgrades to a small number of U.S. communities willing to serve as technology and regulatory "sandbox" testing grounds for autonomous vehicles, drones, and smart city applications. With a revitalized federal smart cities initiative, U.S. agencies could formalize best practice and information sharing on 5G, autonomy, and smart cities technologies between the public and private sectors and state and local governments.

3.4 Digitize U.S. Industry for Networked Applications

Objective: Prepare industrial users to apply 5G and advanced network technologies to their operations.

Method: Expanding broadband connectivity is not enough to allow enterprises to make use of new, 5G-enabled capabilities. Enterprise and industrial uses need basic levels of digital readiness — and the United States should seek to increase digitization and digital skills of strategic industries

in parallel with expansion of private 5G networks.[43] This should encompass tax incentives to defray costs of technology upgrades and workforce training, and increased incentives for sharing best practices within industries, in conjunction with Manufacturing USA[44] and the NIST Manufacturing Extension Partnership (MEP)[45] programming.

3.5 Release More Spectrum for Network Innovation

Objective: U.S. authorities must make more radio spectrum available, not only for telecom networks but also for smaller firms and private and city-scale networks and testbeds. Making more licensed and unlicensed spectrum available to the private sector will be crucial to future economic as well as development of dual-use and security-focused applications.

Method: The FCC's ability to auction and license spectrum to the private sector lapsed March 9, 2023 for the first time in three decades, adding uncertainty to a process that takes years to manage.[46] Congress should offer a long-term or indefinite extension of the FCC's spectrum auction authority.

- With auction authority approved, the FCC and Congress should focus on quickly licensing mid-band spectrum to the private sector, offering the ideal combination of distance and data carrying capacity for public 5G networks to unlock 5G applications across these networks.[47]
- Policymakers should also improve incentives for government agencies to release more spectrum needed for wireless innovation[48] — both by increasing the costs for holding unused spectrum and improving incentives for optimizing spectrum use. The Department of Defense, the government's largest spectrum user,[49] should work closely with the FCC and NTIA to assess its spectrum use and develop a spectrum release strategy to address future economic and security demands of network technology, ensuring the needs of warfighters and innovators are both met.

3.6 Expand the Citizens Broadband Radio Service (CBRS)

Objective: Expand access to unlicensed spectrum for private networks.

Method: The FCC should explore expanding this program to facilitate more private networks, which would be the quickest way to make more spectrum available commercially, and pursue stronger spectrum access guarantees, higher power limits, or other improvements to the CBRS program.[50] The United States has staked out an advantage relative to its competitors by releasing more unlicensed spectrum than any other country in the world,[51] allowing multiple private network operators to access low-cost spectrum across shared bands, which policymakers should seek to harness to spur more distributed network and application innovation.

3.7 Drive More Spectrum Sharing and Efficiency with AI

Objective: Support large-scale research and testing of spectrum sharing technology.

Method: Even with necessary new spectrum allocations, the rapid increase in networked, wireless applications in 5G and 6G — and the consequent need for spectrum[52] — calls for new spectrum sharing techniques and higher efficiency.

The United States should aim to lead the world in researching and adopting AI-driven spectrum sharing techniques to maximize usage efficiency in an increasingly crowded spectrum landscape.

ACTION PLAN RECOMMENDATION | 4 / 4

Shaping Networks Globally: Exportable Network Solutions and Standards

- 4.1 Establish a Tech Export Accelerator
- 4.2 Let EXIM and DFC Lend More Flexibly for Strategic Technology
- 4.3 Build Long-Term Network Technology Cooperation
- 4.4 Flood the Zone in Standards Discussions
- 4.5 Free 6G Leadership Group

The United States has called out the risks of PRC exports of digital infrastructure,[53] which typically facilitate autocratic technology governance practices that threaten the open Internet and democratic values. Yet foreign partners are also seeking alternatives to PRC offerings, and no U.S. firms are major competitors for building integrated telecom networks abroad. The United States does, however, boast world-leading producers of exportable cloud, satellite, subsea and terrestrial fiber optic, and other digital infrastructure technology that — if harnessed, packaged, and financed effectively — could help "offset" that absence. The U.S. Government has taken steps to support strategic technology sales to foreign partners, such as the U.S. Export-Import Bank's (EXIM) policy to support 5G network exports[54] — but more must be done. The United States and its allies must step up efforts to build digital networks in "swing states" – emerging and developing economies that are not closely aligned with either the PRC or the United States.

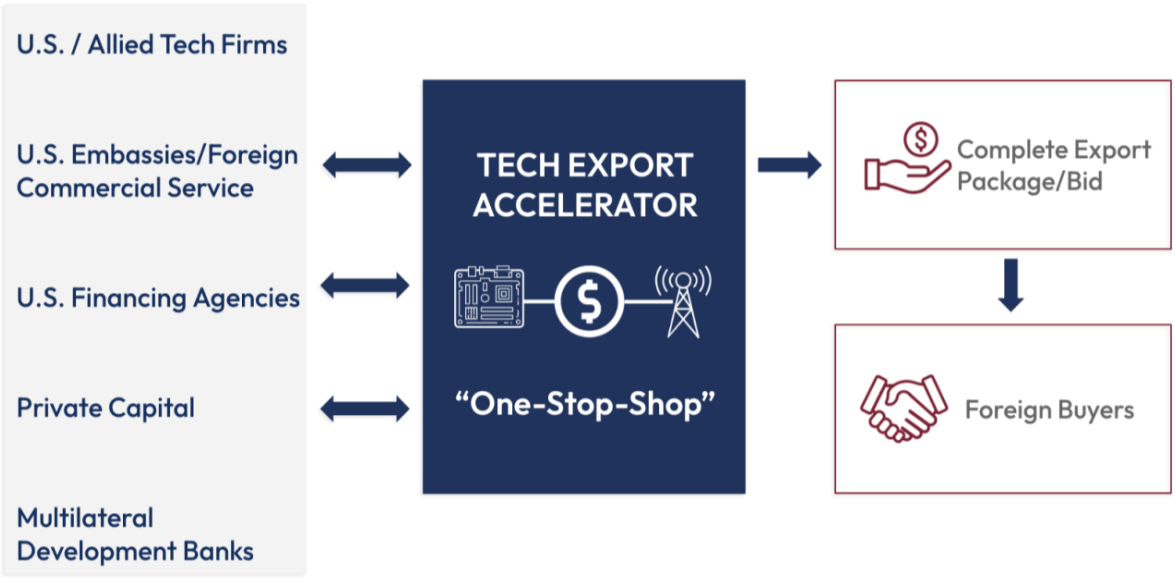
Further action is needed to position U.S. and allied country firms for success: companies and foreign buyers struggle to navigate U.S. government incentive programs due to a lack of agility, coordination, and a complex web of restrictions.

U.S. stakeholders must also strengthen coordination with representatives from democratic and other like-minded countries on developing standards and guardrails for future network paradigms — notably 6G — even as commercial competition among these countries heats up.

4.1 Establish a Tech Export Accelerator

Objective: Create a one-stop-shop to link foreign buyers, U.S. tech exporters, and U.S. agencies to promote trusted digital infrastructure abroad.[55]

Method: A Tech Export Accelerator, created as a new, independent entity in or out of government, should support U.S. government efforts to pursue strategic technology export and investment opportunities, galvanizing U.S. financing agencies, commercial promotion, and diplomatic advocacy tools to structure and win international tenders in partnership with U.S. technology firms. Tech export promotion and investment initiatives should expand their focus on 5G networks to include other types of networks, fiber optic cable, cloud and data centers, e-commerce, financial technology, and other services — offering comprehensive network and infrastructure packages.



4.2 Let EXIM and DFC Lend More Flexibly for Strategic Technology

Objective: Allow U.S. financing agencies to support more network and digital infrastructure exports and investments abroad.

Method: The U.S. Export-Import Bank and U.S. International Development Finance Corporation (DFC) face numerous restrictions on their financing, preventing them from supporting strategic digital infrastructure projects abroad.[56] Common sense changes can be made to allow more financing while still protecting U.S. taxpayers. Congress should allow EXIM and DFC to lend concessionally to buyers and partners based in developing countries for strategic exports and investments; assume more risk in their portfolios to allow financing with existing resources; work with state-owned enterprises in select partner countries; and expand "blended" public-private financing pools.

4.3 Build Long-Term Network Technology Cooperation

Objective: U.S. agencies should foster long-term technology cooperation ties with foreign partners, assisted by U.S. firms, through joint research, development, and training on network technology. For example, USAID has recently sponsored an Open RAN academy[57] and interoperability lab[58] in the Philippines to develop workforce skills and best practices in line with U.S. telecom developments.

Method: Such programs should be developed across many more countries to strengthen tech and human ties, shape technology development abroad, and support the development of key technologies for domestic use.

4.4 Flood the Zone in Standards Discussions

Objective: Assert U.S. public and private sector leadership in international network technology standards setting bodies to guide network standards. The PRC has organized its firms to show up in force in these bodies and speak with a united voice to advance its political objectives.[59]

Method: U.S. standards agencies like NIST should develop a clear strategy for 6G and forthcoming network standards to help support — not replace —the industry-led standards setting process as part of its implementation of the "National Standards Strategy for Critical and Emerging Technologies."[60] The government should also increase support for U.S. firms to participate in these standards setting processes to ensure U.S. perspectives are fully represented. To do this, Congress could expand the research and experimentation tax credit to allow firms to count international standards setting costs towards the credit.[61]

4.5 Free 6G Leadership Group

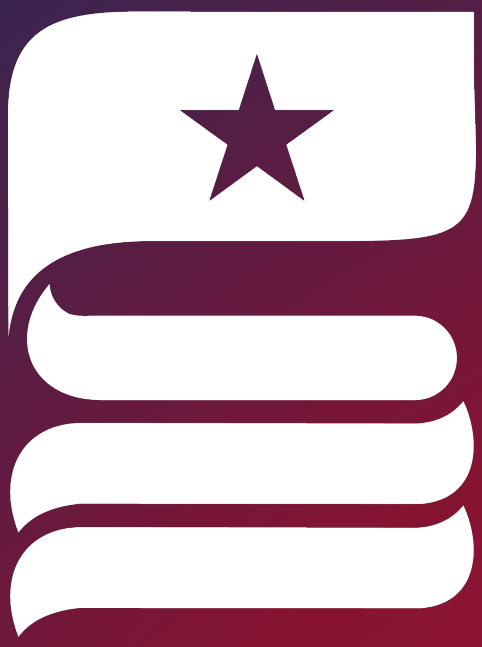
Objective: Build a united effort with allies and partners to guide the development of 6G technology in line with democratic values.

Method: In concert with private sector-led efforts like the NextG Alliance,[62] the U.S. government and other advanced democracies should form a "Free 6G Leadership Group" to support proactive leadership in development of 6G network standards and principles for use cases. U.S. and European governments have begun discussing 6G within the U.S.-EU Trade and Technology Council (TTC). [63] These stakeholders should expand engagements to include Japan, Australia, and India – which have created an Open RAN-focused working group within the Quad[64] – and other partner countries.

Endnotes

[1] Graham Allison & Eric Schmidt, China's 5G Soars Over America's, Wall Street Journal (2022); John McCormick, et al., Huawei, Ericsson or Nokia? Apple or Samsung? U.S. or China? Who's Winning the 5G Races?, Wall Street Journal (2021).
[2] Jon Pelson, Wireless Wars: China's Dangerous Domination of 5G and How We're Fighting Back, BenBella Books at 4-6 (2021).
[3] Liza Tobin, China's Brute Force Economics: Waking Up from the Dream of a Level Playing Field, Texas National Security Review at 81-98 (2022/2023).
[4] Robert D. Atkinson, Who Lost Lucent?: The Decline of America's Telecom Equipment Industry, American Affairs (2020).
[5] Stefan Pongratz, Worldwide Telecom Equipment up 3 Percent in 2022, Dell'Oro Group (2023); Stefan Pongratz, What is the state of U.S. RAN and non-RAN suppliers?, Fierce Wireless (2023).
[6] Huawei Technologies Co., Ltd. and 68 non-U.S. affiliates of Huawei were added to the Entity List in 2019. 84 Fed. Reg. 22961, Addition of Entities to the Entity List, U.S. Bureau of Industry and Security (2019).
[7] Huawei was restricted from certain foreign-produced items that were the direct product of certain U.S. technology or software. 85 Fed. Reg. 51596, Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule), U.S. Bureau of Industry and Security (2020).
[8] FCC Bans Authorizations for Devices That Pose National Security Threat, Federal Communications Commission (2022).
[9] Robert Strayer, U.S. Policy on 5G Technology, U.S. State Department (2019).
[10] Pub. L. 116-124, Secure and Trusted Communications Networks Act of 2019 (2020); Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, Federal Communications Commission (last accessed 2023).
[11] Supply Chain Program Reimbursement Report, Federal Communications Commission (2023).
[12] Biden-Harris Administration Launches $1.5 Billion Innovation Fund to Develop a More Competitive and Diverse Telecommunications Supply Chain, National Telecommunications and Information Administration (2023).
[13] Rick Switzer, The Next Pandemic Could Be Digital: Open Source Hardware and New Vectors of National Cybersecurity Risk, Special Competitive Studies Project (2023).
[14] David Lin, et al., Building a National Delivery System for Data, Special Competitive Studies Project (2023).
[15] David Dorman, China Sees Foreign Threat from Low-Orbit Broadband Satellite Networks; Russia-Ukraine War Increases Urgency, Digital China Wins the Future (2022).
[16] Jonathan E. Hillman, U.S. at Risk of Losing Cloud Computing Edge to China, Politico (2021). On China's ambitions to harness advanced networks to conduct "intelligentized warfare," see Offset X: Closing the Deterrence Gap and Building the Future Joint Force, Special Competitive Studies Project at 6 (2023).
[17] Positive progress by allies should neither be ignored nor overstated. A positive direction still must overcome hurdles of legacy investments. See e.g., Louis Westendarp, Germany Signals a Pivot from China's Huawei, Politico (2023); Iain Morris, Ericsson to replace Huawei at T-Mobile Netherlands, Light Reading (2022).
[18] FSONs operate as laser pulses in open space. FSONs promise faster data transmission and greater security than radio waves, and do not require radio spectrum or fiber build outs — constraints and cost for other network types. Joost Verberk, Free-Space Optics Surpasses Traditional Technology, Laser Focus World (2022).
[19] Sandra Erwin, Military agency praised for leading the way on laser communications, Space Development Agency (2023).
[20] Space-Based Adaptive Communications Node (Space-BACN), Defense Advanced Research Projects Agency (last accessed 2023).
[21] Public Wireless Supply Chain Innovation Fund, National Telecommunications and Information Administration (last accessed 2023); Sec. 106 of P.L. 117-167: $150m for FY 22-31; $1.35b for FY 23-32 (last accessed 2023).
[22] Muhammad Waseem Akhtar, et al., The Shift to 6G Communications: Vision and Requirements, Human-Centric Computing and Information Sciences (2020).
[23] National Cybersecurity Strategy, The White House (2023).
[24] Liza Tobin, China's Brute Force Economics: Waking Up from the Dream of a Level Playing Field, Texas National Security Review (2022/2023).
[25] A DemTech Agenda: Ten Steps Towards Collective Resilience, Special Competitive Studies Project (2023).
[26] Rick Switzer, The Next Pandemic Could Be Digital: Open Source Hardware and New Vectors of National Cybersecurity Risk, Special Competitive Studies Project (2023).
[27] In addition to the measures enumerated here, see also the recommendations in SCSP's Economy Panel Interim Panel Report related to PRC telecom firms, at 74-75.
[28] Fact Sheet: Department of Commerce's Use of Bipartisan Infrastructure Deal Funding to Help Close the Digital Divide, U.S. Commerce Department (2021).
[29] Robert D Atkinson, How Applying 'Buy America' Provisions to IT Undermines Infrastructure Goals, Information Technology & Innovation Foundation (2022).
[30] Department of Defense Hosts Ribbon-Cutting for 5G Smart Warehouse Network, U.S. Department of Defense (2022).
[31] List of Equipment and Services Covered By Section 2 of The Secure Networks Act, Federal Communications Commission (last accessed 2023).
[32] Secure and Trusted Communications Networks Reimbursement Program Report, Federal Communications Commission (2023).

[33] Middleware provides a software between operating systems and the applications that run on them. See Michele Polese, et al., Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges at 17, IEEE (2021).
[34] Shalanda D. Young, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, U.S. Office of Management and Budget (2022). This requirement, which will go into effect on June 12, 2023, carried out a recommendation issued in a 2021 Executive Order. See Executive Order on Improving the Nation's Cybersecurity, The White House (2021); Jeffrey A. Koses & David A. Shive, Memorandum for the GSA Acquisition Workforce: Ensuring Only Approved Software is Acquired and Used at GSA, General Services Administration (2023).
[35] Rick Switzer, The Next Pandemic Could Be Digital: Open Source Hardware and New Vectors of National Cybersecurity Risk, Special Competitive Studies Project (2023).
[36] Karen Campbell, et al., The 5G Economy, IHS Markit at 4 (2019).
[37] Is Your Technology Moving Fast Enough to Realize Your Ambitions? EY Reimagining Futures Study 2023 at 7, EY (2023).
[38] The Challenge of Monetizing 5G, PwC (2023); Sandra Vogel, Why 5G Monetisation is Proving a Headache for Operators, ITPro (2022).
[39] Suman Bhattacharyya, Telecom Companies Pin 5G Hopes on Private Industrial Networks, Wall Street Journal (2023) (citing a 2022 Gartner survey of 2,203 CIOs and technology executives).
[40] Jon Pelson & Warren Wilson, Round Two of the 5G Battle is Just Beginning. Can America Surge Ahead?, Special Competitive Studies Project (2023).
[41] 5G Challenge, National Telecommunications and Information Administration (last accessed 2023).
[42] Platforms for Advanced Wireless Research, Platforms for Advanced Wireless Research Program (last accessed 2023).
[43] Automation Across Industries, Special Competitive Studies Project (2023).
[44] Manufacturing USA (last accessed 2023).
[45] NIST Manufacturing Extension Partnership, National Institute of Standards and Technology (last accessed 2023).
[46] Jill C. Gallagher & Patricia Moloney Figliola, FCC Spectrum Auction Authority: Background and Proposals for Extension, Congressional Research Service (2022).
[47] Mid-Band Spectrum Update, 5G Americas at 5 (2023).
[48] Joe Kane & Jessica Dine, Building on Uncle Sam's "Beachfront" Spectrum: Six Ways to Align Incentives to Make Better Use of the Airwaves, Information Technology & Innovation Foundation (2023).
[49] John R. Hoehn, et al., Overview of Department of Defense Use of the Electromagnetic Spectrum, Congressional Research Service at 5 (2021).
[50] 3.5 GHz Band Overview, Federal Communications Commission (last accessed 2023).
[51] Janette Stewart, et al., Comparison of Total Mobile Spectrum in Different Markets, Analysys Mason (2022).
[52] Coleman Bazelon & Paroma Sanyal, How Much Licensed Spectrum Is Needed to Meet Future Demands for Network Capacity?, Brattle Group for CTIA at 9 (2023).
[53] Robert L. Strayer, U.S. Policy on 5G Technology, U.S. State Department (2019).
[54] Export-Import Bank of the United States' Board of Directors Approves Clarified Policy for 5G Transactions, U.S. Export-Import Bank of the United States (2023).
[55] Restoring the Sources of Techno-Economic Advantage, Special Competitive Studies Project at Appendix D (2022).
[56] Eligibility Checklist, U.S. International Development Finance Corporation (accessed 2023); EXIM Bank Policies, Export-Import Bank of the United States (last accessed 2023).
[57] Mayumi Hirosawa, U.S.-Japan 5G Initiative launches First Academy in Philippines, Nikkei Asia (2022).
[58] United States Announces $135 Million to Advance a Prosperous, Inclusive, and Resilient Philippines, U.S. Agency for International Development (2023).
[59] Daniel R. Russell & Blake H. Berger, Stacking the Deck: China's Influence in International Technology Standards Setting, Asia Society Policy Institute (2021).
[60] United States Government National Standards Strategy for Crucial and Emerging Technology, The White House (2023).
[61] Robert D. Atkinson & Martijn Rasser, Help US Companies Compete Against China on Technology Standards, RealClear Policy (2022).
[62] Next G Alliance, Next G Alliance (last accessed 2023).
[63] U.S.-EU Joint Statement of the Trade and Technology Council, The White House (2022).
[64] Statement on the Quad Leaders' Tokyo Summit 2022, Open RAN Policy Coalition (2022).



SCSP.AI