Policy Report

March 2023

The New American Foreign Policy of Technology

Promoting Innovation, National Security, and Democratic Values in a Digital World

Karen Kornbluh and Julia Tréhu

GMF
Ideas.
Leadership.
Hope.

75 The Marshall Plan 1947–1951
GMF 50

SUMMARY

Laissez-faire globalization is at the breaking point. The COVID-19 pandemic and Russia's invasion of Ukraine finally exposed the fragility of the global economic system after decades of strain caused by the rise of China, and exacerbated by climate change and growing inequality. Now, US leadership is needed to ensure that nationalist and authoritarian forces do not fill the resulting structural vacuum in an increasingly digital world. A new roadmap is needed for how democracies and their allies will address the technological challenges of the 21st century.

Progress has begun. In its first two years, the Biden administration has ushered in a new strategy of industrial policy that includes tens of billions of dollars in technology subsidies. Meanwhile, Europe is pursuing its own Chips Act to boost domestic semiconductor research, development, and production. Together, the transatlantic partners have imposed tough controls on technology exports to Russia and China.

These new policies hold great promise for building more resilient supply chains, creating jobs, and safeguarding national security. Yet the current international economic system is not fit for purpose. The US's new industrial policy faces accusations of protectionism from allies and competitors. Europe objects to provisions in new clean-energy subsidies, and China has accused the United States of the "weaponization and politicization" of science and technology "to maliciously block and suppress Chinese companies".

This backlash risks undermining US efforts to lead on global rules and values. The US must have its allies' support for addressing technology challenges, from restricting Chinese access to critical semiconductor technology to contesting efforts in standards organizations to approve surveillance technologies. All this must be done in the name of promoting global rules and defending democratic principles and values. Yet questions have emerged about whether a geopolitical digital approach is compatible with the United States' traditional defense of an open, global internet and human rights more generally.

Domestically, new US public spending must not crowd out entrepreneurs and innovators, but it must include guardrails to ensure that offline protections and rights apply online. The ecosystems that produce advances in biotechnology, ensure that citizens in repressive countries have access to information, and underpin globally interconnected semiconductor manufacturing require careful nurturing through partnerships with the private sector. A top-down approach will not succeed.

To resolve all these tensions, the United States must plug gaps in the old, 20th-century system with new multistakeholder institutions for the digital age. These building blocks would constitute a new technology policy architecture to support socially responsible innovation and digital trade. A new foreign policy of technology comprising three key parts is needed to build this new architecture:

- Nurturing innovation through a **Digital Policy Lab**: The lab would serve as a platform for domestic public-private-civil society partnerships that would further government capacity-building, agile investment coordination, and development of clear guardrails to enable innovation and democratic accountability.
- Enabling resilient allied supply chains (or "friend-shoring") by creating a new international **Technology Task Force** would deepen cooperation among democracies and allies. Joint action should start by focusing on semiconductors, green technologies (e.g., electric vehicles), and critical minerals. The task force would act like the International Energy Agency, which

was built by Organization for Economic Co-operation and Development (OECD) member countries responding to the Organization of the Petroleum Exporting Countries' (OPEC) oil cartel. It would make available supply and demand data for planning purposes, coordinate responses to shortages or vulnerabilities, including the introduction of subsidies, and provide a venue for countries to reconcile export controls and secure technology standards in areas such as 5/6G.

- Defending digital democracy by promoting internationally the principles in the **Declaration for the Future of the Internet**, a commitment signed by 61 countries promising to uphold an "open, free, global, interoperable, reliable, and secure Internet". This would renew a commitment to a broader conception of internet freedom through ongoing efforts to adopt complementary internet guardrails and hinder internet shutdowns, censorship, surveillance, information operations, and cyberattacks.

BACKGROUND

The globalization that emerged in the aftermath of the Cold War failed to respond to authoritarian transgressions or global crises. The United States saw capitalism's advance and the global adoption of the internet as signs that unfettered globalization would multiply opportunity. It optimistically invited China into the trade tent without demanding that Beijing adhere to democratic standards and trading system norms. It also simultaneously reduced domestic investment in research and development (R&D) and infrastructure, and allowed even critical technologies to be produced overseas.

Over time, China and Russia each weaponized the trading system to its own benefit and to the detriment of Western societies and the global order. China subsidized its technology champions and leveraged access to its market while manipulating international standard-setting organizations. Online, it stole intellectual property and personal data, joining Russia in launching information operations. Russia also harbored ransomware attackers. Both countries turned technology against their own citizens and supported repressive regimes worldwide.

Even so, debates in the West about whether and how to "decouple", or restrict economic ties with China, wrestled with the intense interdependence of the global trading system. The mounting abuses of globalization posed an apparent paradox: Was it possible to protect the open, rules-based system from authoritarians without damaging Western countries—vulnerable because of their very openness—and without sacrificing the openness of the system itself?

The Trump administration's strategy was to walk away from trade deals negotiated during the Obama era that were meant to strengthen relations with Asia. It also took various unilateral actions, including erecting tariffs on more than $200 billion of Chinese goods and imposing additional tariffs on steel and aluminum imports from every country but Canada and Mexico. It broke off international tax negotiations at the OECD, leading France and the United Kingdom to impose digital taxes to which the United States responded with more of its own tariffs. And, of course, the United States pulled out of the Paris Climate Agreement, protesting that the deal would be bad for US industry and good for China.

To the surprise of many, although the Biden administration repudiated the go-it-alone America First approach, it did not return to laissez-faire globalization.

The "America First" trade approach rejected the old model of globalization but did not advance a positive agenda to strengthen supply chains. It also eroded critical alliances. A resolution adopted by a large margin (490-148) in the European Parliament in September 2018, for example, criticized America First policies as undermining mutual trust with "unilateral moves [that] only weaken the transatlantic partnership". The administration was more successful in working with allies to slow the cybersecurity risk of Chinese telecommunications company Huawei's expansion into Western networks.

To the surprise of many, although the Biden administration repudiated the go-it-alone America First approach, it did not return to laissez-faire globalization. It rejected both concepts, pursuing instead what the National Economic Council calls a "modern industrial policy" and the National Security Strategy terms an "allied techno-industrial base". The new agenda includes revitalizing domestic manufacturing by enacting tens of billions of dollars in subsidies to strengthen the US technology base along with additional tough sanctions and export controls to deny Russia and China access to critical technology.

The strategy also entails efforts to repair international relationships by working with partner countries on export controls and launching regional economic alliances, including the EU-US Trade and Technology Council, the Americas Partnership for Economic Prosperity, and the Indo-Pacific Economic Framework for Prosperity.

This new strategy, however, remains a work in progress. Efforts to find agreement—on climate, digital taxes, technology regulation, and semiconductors—have proved especially difficult. Without additional refinement, the US approach risks forcing zero-sum choices:

- **National security and industrial policy vs. innovation:** Public investment runs the risk of picking winners and losers. Building national technology assets depends on whether private-sector innovation—in areas such as artificial intelligence (AI), biotech/genomics, and quantum computing—is also nurtured.
- **Strengthening domestic industry vs. working with allies:** The United States cannot afford to alienate Europe and other partners, especially as it seeks to create resilient supply chains. In fact, the recently released National Security Strategy commits to building a "allied techno-industrial base".
- **A more muscular geopolitical approach to technology competition vs. the global open rules-based system**: As the United States confronts Chinese and other authoritarian efforts, it must clarify how doing so is in support of, and not in opposition to, the multilateral system.
- **Defending interests online vs. safeguarding rights and internet freedom:** As the United States takes a more muscular approach to defending its online interests, it cannot abandon freedom of speech, association, and online security, at home or abroad, in the face of growing digital authoritarianism.

Addressing the tensions inherent in these four sets of options will be crucial to crafting a new and durable foreign policy of technology.

NURTURING US INNOVATION

As the United States builds an industrial policy, it must ensure it cultivates rather than undermines the innovation ecosystem that is its source of strength. This delicate ecosystem cannot be weakened as the US strives to respond to China and authoritarian threats.

Concern about Chinese weaponization of the global trading system to gain advantage is behind the bipartisan support for the CHIPS Act and export controls. National Security Advisor Jake Sullivan has warned that "our competitors and adversaries took advantage of our complacency and inherent openness". Republican Senator Todd Young explained his support for the act and role in bringing Republican colleagues on board by noting that semiconductor "technologies are key to [US] national security". Central Intelligence Agency Director Bill Burns agrees that technology is the "main arena for competition and rivalry with China".

While the United States remains the global leader in R&D, China's subsidization of its national champions, forced technology transfer, and theft of intellectual property have helped it close the gap. Its "Made in China 2025" strategy and related plans set out a roadmap for continued efforts in these areas.

China has become the world's top high-tech manufacturer and a serious competitor in key technologies. According to the Belfer Center, the United States still leads in breakthrough AI innovations, but China leads in implementation. To strengthen US capabilities, the Department of Defense established a Joint AI Center, but a General Accounting Office report found the Pentagon's AI-related strategies could be more comprehensive. Thanks, in part, to billions in government support, China surpassed the United States in quantum communication and has already built a quantum communications network from Beijing to Shanghai. And while the United States continues to dominate in biotechnology, it risks losing its edge to China, whose military-civil fusion strategy explicitly highlights that field as a priority. China has already made significant advances in biotechnology R&D, for example in human genome sequencing, therapeutics, and the CRISPR gene-editing technique (which led to scandal).

China is also the world's leading manufacturer, user, and exporter of green technologies, making US industry interdependent with China's.

China is also the world's leading manufacturer, user, and exporter of green technologies, making US industry interdependent with China's. Ninety-seven percent of the world's production of silicon wafers for solar photovoltaic cells occurs in China, while about 75% of the silicon solar cells incorporated into panels installed in the United States are made by Chinese subsidiaries in Vietnam, Malaysia, and Thailand. China dominates manufacturing of magnets used in wind turbines. It controls 61% of global lithium refining, which is key for battery storage and electric vehicles. Seventy percent of the global supply of cobalt for lithium-ion batteries comes from mines in the Democratic Republic of the Congo, a significant portion of which is owned by Chinese companies. China has 100% of the processing of natural graphite used for battery anodes. It controls 80% of rare-earth elements production and refining, which are critical for components in technologies such as wind turbine direct drive generators. These elements include neodymium for offshore wind and electric vehicle motors, platinum group metals for catalysts, tellurium for solar photovoltaics, and uranium for nuclear energy. Substitution is difficult due to the unique characteristics and technical

Table 1. Simplified Accounting of Current Advantage, United States and China

	United States	China
AI	●	●
5G		●
QIS	●	
Semiconductors	●	
Biotech	●	
Green energy	●	●

advantages of rare-earth elements. Global efforts to accelerate green technology adoption to tackle climate change must grapple with this interdependency.

As a result of large subsidies for Huawei, China's 5G infrastructure rollout is well ahead of that in the United States. And the future looks troubling: The United States has advantages in 5G standards and chip design, but China already holds 35% of 6G patents compared to the United States' 18%. The US rollout of 5G has also been uneven, in part due to supply chain problems. An Open Radio Access Network is a response to market concentration and lack of diversity in network equipment, but its rollout requires a reliable supply of trusted, technically viable parts and software.

In the key area of semiconductors, the United States and the EU remain leaders in the most intensive R&D activities including chip design and underlying software development, and in essential chip-making machinery, such as Lam Research's plasma etching machines, Applied Materials' eBeam metrology system for semiconductor patterning control, and ASML's extreme ultraviolet lithography systems. The most advanced computer chipmaking equipment and chips rely largely on US intellectual property even if they are manufactured overseas. The United States lacks the appropriate manufacturing facilities and, though allies account for the majority of chip production (Taiwan supplies the United States with 90% of its most advanced chips, and South Korea supplies the remaining 10%), their proximity to China is a matter of concern.

The United States is responding by launching an industrial policy, a concept considered anathema for decades.

To its credit, China also invests in its building blocks for innovation, including R&D. The country now graduates more science, technology, engineering, and math doctorates than the US, and the gap is projected to widen. Chinese university funding has doubled since the early 2010s, especially for the most elite institutions. And Chinese students consistently outscore their American counterparts in math and science testing, according to the OECD.

The United States is responding by launching an industrial policy, a concept considered anathema for decades. National Economic Council Director Brian Deese says the administration's new public spending "means that rather than accepting as fate

that the individualized decisions of those looking only at their private bottom lines will put us behind in key sectors, we engage in strategic investment in those areas that will form the backbone of our economy's growth over the coming decades, areas where we need to expand the nation's productive capacity".

The move toward US public investment, at least in part, has bipartisan support. Congress and the president enacted the $280 billion bipartisan CHIPS and Science Act that provides:

- $52.7 billion to incentivize semiconductor manufacturing capacity
- $81 billion over five years (a $36 billion increase) for the National Science Foundation to establish a new directorate for technology, innovation, and partnerships to focus on AI, 5/6G and quantum computing, and to increase its university and startup funding
- $10 billion over five years for the National Institute of Standards and Technology (NIST) to establish a National Semiconductor Technology Center and an Advanced Packaging Manufacturing Program to bridge the gaps between public and private investments and expand capacity across the semiconductor chain from R&D to testing and assembly
- $11 billion over five years for regional technology hubs
- $166 million over five years for a new program that facilitates research on quantum computer capacity, and $500 million to the Department of Energy to expand national quantum infrastructure

Other public investment includes:

- The Inflation Reduction Act's (IRA) nearly $370 billion in climate spending
- The Infrastructure Investment and Jobs Act's $65 billion for broadband and digital inclusion
- The $2 billion National Biotechnology and Biomanufacturing Initiative for strengthening supply chains, manufacturing, and R&D

Table 2. Estimated Share of Global R&D Expenditures (in percent)

	2000*	2020**
United States	40	31
China	5	25
Japan	15	7
Germany	8	6
South Korea	3	5

*Note: * total global R&D spending $725 billion. ** total global R&D spending $2.352 trillion*
Data drawn from: "Research and Development, U.S. Trends and International Comparisons," National Science Foundation, January 2020; "Global Research and Development Expenditures: Fact Sheet," Congressional Research Service, September 14, 2022.

Implementation of the funding will require cooperation among various stakeholders including federal, state, and local governments, the private sector, labor, and civil society. It will also require transparency and clearly defined goals. Government has a long history of investing in key industries, including in critical technology sectors. But firestorms, such as those generated when Solyndra defaulted on a loan guaranteed by the Obama administration's Energy Department (as part of a program that eventually turned a profit), reflect the challenge of explaining to the public the government's role.

Stakeholders' functions depend on specific goals. For deploying enabling technologies, including broadband, the government role is funding and coordinating with communities. For ensuring resilient supply chains of critical technologies, such as semiconductors and clean energy, the government role entails export controls and funding and coordinating with industry, communities, and labor. For emerging technologies, such as bioengineering, however, the government should create platforms for innovation by focusing on R&D funding and setting appropriate guardrails.

To play these enabling roles, the government must build its own capacity, coordinate new projects across federal agencies, and confront baroque and under-resourced permitting procedures. Flawed cost-benefit analyses and lengthy regulatory processes, as well as outdated purchasing systems, pose additional obstacles to reform. Congressional budget rules and conventions will also constrain investment initiatives.

The United States must also avoid the trap of failing to update regulations out of fear that doing so will create an advantage for rivals.

The United States must also avoid the trap of failing to update regulations out of fear that doing so will create an advantage for rivals. The lack of updated privacy protections, for example, is not only a national security vulnerability that allows foreign governments to buy data on Americans. Outdated protections also permit other countries, notably European, to lead, and they limit the data sharing needed to fuel advances in AI. The United States is similarly lagging in platform regulation, competition, and AI, but proper guardrails can spur productive innovation.

Nurturing this innovation requires a multistakeholder **Digital Policy Lab** comprising:

- Capacity building: The administration has handed White House coordinators responsibility for the Infrastructure Act, clean-energy spending, and semiconductor strategy. Civil servants with the appropriate technical skills will need to be hired or trained, and must work with stakeholders outside government.
- Strategic funding: Government must work with industry to develop strategic frameworks for targeting funding where it is necessary (e.g., science and R&D with relatively low rates of return, high-risk or enabling projects, national security priorities). Metrics must be developed for evaluation and reporting progress to the public and to industry, and to inform an agile funding process. Permitting processes must be properly resourced and updated.
- Data platforms: Empirical evidence should be used over the longer term to reform budget rules and the cost-benefit calculus used to evaluate funding and regulations, and to account for the growth that investment generates. Additionally, a handbook for permitting reforms, moonshots, advanced purchase commitments, regulatory sandboxes, co-regulation, and other procedural reforms is needed. The same is true for a federal privacy law that would enable the safe sharing of personal data and, consequently, advances in AI for the medical and other critical sectors.
- Agile regulation: Audits can enable rigorous accountability without curbing innovation. GMF has proposed algorithmic audits with clear standards, such as those for financial accounting to avoid white washing (or "audit washing", according to a GMF Digital report).

"FRIEND-SHORING"

The IRA, which the Biden administration negotiated with Congress and which contains tax credits for electric vehicles, requires that two-fifths of the critical minerals used in electric vehicle batteries be extracted and processed in the United States, with exceptions only for free trade agreement partners (a group of 20 countries that excludes Europe), or have been recycled in North America. The threshold could be raised to 80% in 2026. These stipulations, however, are in tension with an executive order on "friend-shoring". That order noted that "close cooperation on resilient supply chains with allies and partners who share our values will foster collective economic and national security and strengthen the capacity to respond to international disasters and emergencies".

Unsurprisingly, a senior South Korean official called the critical minerals requirement a "betrayal", and French President Emmanuel Macron threatened "Buy European" provisions. European Commissioner for Trade Valdis Dombrovskis said the EU will monitor US procurement rules to determine if they contravene World Trade Organization (WTO) commitments. The European Commission is preparing a "Green Industrial Plan" as a response to the IRA. That comes on top of the EU's updating its International Procurement Instrument to let it shut out companies from countries that have barred its companies.

The IRA debate also occurs as Europe is increasingly intent on what is often referred to as "digital sovereignty". European High Representative Josep Borrell, in a speech to EU ambassadors, castigated the bloc for having "delegated our security to the United States", and warned that the EU "need[s] to shoulder more responsibilities ourselves" since a world in which the United States provided security, while China and Russia provided markets and energy, "is no longer there".

The United States and the EU have said they will work together to avoid a "subsidy war" on semiconductors, but ongoing diplomacy will be necessary there as well. The EU's Chips Act, scheduled for adoption in 2023, promises to mobilize €43 billion in investment across the semiconductor supply chain, from R&D to leading-edge manufacturing and workforce initiatives.

The Transatlantic Roots of Leading-Edge Chip Manufacturing

The Dutch company ASML—the leader in lithography machinery and sole supplier for leading-edge chip manufacturing—is a transatlantic success story. Initial research on extreme ultraviolet (EUV) lithography technology began in the early 1980s, but no US company has had the capacity to commercialize the technology. ASML belongs to an association that includes the US Department of Energy, Intel, Belgium's Imec Research Center, and the American SEMATECH consortium, and has received direct investment from Intel, Samsung, and Taiwan Semiconductor Manufacturing Company to develop EUV technology. ASML later purchased San Diego-based Cymer, which develops high-powered lasers, and sources mirrors from Germany's Zeiss. However, since 1990, semiconductor manufacturing has moved away from the United States and Europe.

Table 3. Semiconductor Global Manufacturing Capacity (by location, in percent)

	1990	2020
United States	37	12
Europe	44	9
Taiwan	0	22

Source: Antonio Varas, et al., "Government Incentives and US Competitiveness in Semiconductor Manufacturing," Boston Consulting Group and Semiconductor Industry Association, September 2020, 7.

Note: Figures exclude capacity below 5 kwpm, or less than 8 inches.

Taxation

Additional global digital trade tensions arise from tax base erosion. To stem the rise of unilateral responses, the OECD negotiated a two-pillar scheme, which alters the taxation of revenue in markets where multinational enterprises earn profits but lack a physical presence, and which introduces a global minimum corporate tax rate of 15%. The United States enacted a new minimum tax, but it differs from the negotiated structure. The EU reached agreement on implementing a 15% minimum tax after months of negotiation and initial vetoes from Hungary and Poland. But in light of the delays and discrepancies, the OECD secretary-general warned that implementing the new global tax arrangements would be pushed back at least to 2024. In response, European governments warned that, without implementation, they will return to the proposed digital services taxes set aside in 2021 when the OECD process was nearing finalization. This could trigger US retaliation.

Sanctions and Export Controls

In response to Russia's invasion of Ukraine, as Western countries put in place unprecedented sanctions and export controls on high-tech equipment to restrict Russia's long-term ability to innovate, the United States reached for the Foreign Direct Product Rule (FDPR) already deployed against Huawei and its affiliates. This variant on traditional export controls requires licenses for the reexport and transfer of sensitive US-origin items and sensitive foreign-produced items that use US-licensed equipment, software, and plans. When the United States cut off Huawei's access to products made with US equipment, the company, by some accounts, suffered a 30% revenue loss.

The United States worked to deny Russia's entire defense, aerospace, and maritime sectors access to semiconductors, software and hardware for quantum computing, telecommunication devices, encryption security, lasers, sensors, navigation, avionics, maritime technologies, and oil and gas refining equipment. The United States also applied financial sanctions against Russian telecommunications networks, technology firms, and malicious cyber actors.

A common licensing policy was quickly adopted by 38 countries to deny these organizations access to a host of dual-use and other items. Taiwan Semiconductor Manufacturing Company (TSMC) stated that it would abide by all export control regimes.

US companies from Apple and HP to software and cloud providers—such as Microsoft, Oracle, Amazon Web Services, and Google Cloud—joined the bandwagon by withdrawing, at least partially, from Russia. They ceased sales of new products and

services, though some still provide existing customers with select services. Major semiconductor suppliers Intel, Nvidia, AMD, and TSMC suspended sales to Russia.

The United States built on the coordinated response to Russia's aggression to act against China as well, and Washington's overarching strategy soon became apparent. As National Security Advisor Jake Sullivan explained, "On export controls, we have to revisit the longstanding premise of maintaining 'relative' advantages over competitors in certain key technologies. We previously maintained a 'sliding scale' approach that said we need to stay only a couple of generations ahead. That is not the strategic environment we are in today. Given the foundational nature of certain technologies, such as advanced logic and memory chips, we must maintain as large of a lead as possible."

The United States added of a number of Chinese technology firms to its Entity List, which imposes additional licensing requirements. The move limited Chinese access to a variety of cutting-edge technologies, including electronic computer-aided software, next-generation chip substrates, advanced chips used in certain quantum computing, and AI produced with US equipment or software. The new approach to export controls is unique not only in its repeated use of the FDPR but also by its significantly lowering the threshold for the types of technology subject to new licensing requirements, and by restricting US persons' ability to "support" high-end chip manufacturing, a policy targeting US nationals or dual nationals at key positions in some Chinese firms. Chinese semiconductor companies subsequently lost $8.6 billion in market value. On top of all that, the Federal Communications Commission announced plans to ban US sales of Huawei and ZTE devices and of video surveillance equipment from Hytera Communications, Hikvision, and Dahua Technology.

Meanwhile, the United States worked to convince allies to join its efforts to deny the Chinese military access to the latest semiconductor technology. Three US suppliers—Applied Materials Inc., Lam Research Corp. and KLA Corp.—alongside Dutch ASML and Japanese Tokyo Electron Ltd. dominate the global chip equipment market. Washington recently reached an initial agreement with the Dutch and Japanese governments on export restrictions for advanced chip-making tools. A public announcement is pending.

Standards

China has been undermining the global standard-setting system by coordinating government and corporate influence of international bodies. The country already sends the largest delegations to International Telecommunications Union (ITU) study groups and has flooded them with proposed specifications and contributions. China's share of International Standards Organization (ISO) secretariats grew from 5% in 2011 to almost 10% by 2022. China leads all nations with standard essential patent applications. In 2022-2024, China will chair 24% of ISO working groups; Japan comes next at 15%. China's Standards 2035 plan creates a blueprint for amping up this strategy.

The US National Security Commission on Artificial Intelligence's final report underlines the importance of promoting privacy-protecting standards and norms, including through international bodies. Accordingly, NIST released its plan for federal engagement in developing technical standards and related tools and AI.

Trade/Alliances

The US government is calling out China for contravening at least the spirit of WTO rules. Secretary of State Antony Blinken noted that "rather than using its power to reinforce and revitalize the laws, the agreements, the principles, the institutions that enabled its success so that other countries can benefit from them too, Beijing is undermining them."

While calling for WTO reform, the United States is building regional economic alliances to work through disputes. The EU-US Trade and Technology Council (TTC) was established to negotiate agreements on a range of key issues, from AI to platform governance to semiconductors, and, especially, to coordinate technology-related sanctions following the Russian invasion.

Through the TTC's ten working groups, EU and US officials have established direct lines of communication and personal relationships that facilitate coordination and exchange. Another new initiative, the Indo-Pacific Economic Framework for Prosperity, addresses issues related to trade, supply chains, energy, infrastructure, taxation, and corruption. A proposed "Chips 4" alliance with South Korea, Japan, and Taiwan to share information and coordinate on supply chains, and avoid subsidy races, has yet to produce results.

To build additional alliances, the US also sees the need to counter China's Belt and Road Initiative, which provided an annual average of $85 billion in development financing from 2013 to 2017, twice that spent by the United States. A new strategy toward sub-Saharan Africa commits to channel investment and promote collaboration on issues from internet access to vaccine development, and a pledge of $40 million to the Association of Southeast Asian Nations leaders aims to help decarbonize the region's power supply and develop digital economy and AI laws. The US Agency for International Development's Digital Democracy Initiative will mobilize an additional $335 million through partnerships to promote finance and internet service provider initiatives in underserved areas such as sub-Saharan Africa. And US Treasury Secretary Janet Yellen announced a contribution of $1 billion to the World Bank's Clean Technology Fund to advance low-carbon technology in developing nations. This comes on top of US Climate Envoy John Kerry's announcement at the 2022 COP27 in Egypt of a new Energy Transition Accelerator that will help mobilize capital investment in clean energy in developing countries.

A new multistakeholder coordinating body would provide trusted means for sharing supply chain data, including information on product sustainability and security.

G7 countries, for their part, have also launched the Partnership for Global Infrastructure and Investment, which mobilizes $600 billion in development finance tools and private investment for projects ranging from energy transition partnerships to submarine cables in low- and middle-income countries.

Despite these efforts to enhance cooperation, a more permanent forum is needed to work with other democracies and allies to build resilient supply chains. When oil-consuming countries needed to confront the OPEC cartel, they formed the International Energy Agency to share data and coordinate strategies, including the management of strategic oil reserves. The Financial Action Task Force similarly coordinates efforts to combat money laundering.

A new multistakeholder coordinating body would provide trusted means for sharing supply chain data, including information on product sustainability and security. Countries would cooperate on targeting subsidies and craft common responses, including export controls. A **Technology Task Force** (TTF) could help coordinate R&D, building on initial semiconductor R&D talks through NIST. The body could also address key questions about foreign participation rules and necessary integration of R&D systems.

The TTF would focus initially on semiconductors and clean technology supply chains, including those for critical minerals and materials sourcing. It could also take up workforce development and immigration rules to address skilled labor shortages, perhaps through a Schengen-like agreement for specific talent categories.

By offering countries access to supply chains and R&D, the TTF would build support for cooperation in other multilateral organizations, including in the ITU's standard-setting bodies to prevent approval of cyber-insecure technologies and those that enable surveillance.

The TTF could use as its foundation the OECD's newly launched Global Forum on Technology and, like the forum, include democracies and other countries willing to cooperate on common norms.

DIGITAL DEMOCRACY VS. DIGITAL AUTHORITARIANISM

China, Russia, and other repressive regimes have weaponized the open internet as they have weaponized the open trading system. China stole intellectual property and personal data. Russia harbored ransomware attackers. Both countries turned technology against their own citizens and supported repressive regimes worldwide doing the same. Information operations grew ever more sophisticated and brazen.

The United States is pushing back but, as with trade, it should not make a false choice between a narrow conception of geopolitics and bolstering an open system, human rights, and democracy. A forward-looking agenda would prioritize the following aspects.

Internet Governance

Russia and China strive to use the UN to rewire the internet so that individual countries can exert more control over information flows. In a joint June 2022 statement, the two countries reiterated their support for a "sovereign internet". Three months later, however, the US candidate for the ITU presidency beat the Russian candidate (who had previously worked for Huawei). The United States built the alliance to defeat him by working with Europe, whose candidate won the deputy secretary general slot. China, which supported the Russian presidential candidate, has focused its energy on filling many of the lower-level positions that make key standard-setting decisions.

At the UN, negotiations began in spring 2022 on a new cybercrime treaty. The aim is to have an agreement in early 2024. Major differences persist, including over the definition of cybercrime and the risks to free expression and human rights posed by some countries' push to include broader definitions of concepts, such as disinformation, within an expanded treaty. While the Budapest Convention that governs cybercrime counts 67 signatory countries, the new UN cybercrime treaty may have broader scope and legitimacy, and enable transnational cooperation.

In the meantime, as part of the "digital blockade" of Russia, the Ukrainian minister of digital transformation requested that the Internet Corporation for Assigned Names and Numbers (ICANN), the multistakeholder policymaking body responsible for maintaining the internet's domain name system, revoke Russian-based domain names and shut down Domain Name System (DNS) servers in Russia. The United States refrained from supporting this request, which was ultimately rejected for "restrict[ing] access against segments of the Internet". ICANN noted that such a move could have long-term effects on trust in the global internet, worsen access to reliable news and expression within Russia, and cause disproportionate harm through blocking access to key services.

Global Data Flows

Data has become a form of global infrastructure, essential for economic growth and digital transformation and innovation. But a lack of multilateral mechanisms for protecting rights hinders data flows and data sharing, and data localization measures are arising worldwide. The new EU-US Data Privacy Framework is the latest effort to resolve tensions over transatlantic data flows. Meanwhile, the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, adopted at the end of 2022, is the first intergovernmental agreement on common approaches to safeguarding privacy and other human rights

and freedoms when national security and law enforcement officials access personal data. A broader multilateral roadmap on data sharing, however, building on these previous agreements and the Global Cross-Border Privacy Rules Declaration, could supercharge the benefits of AI and cloud technologies for security and medical research. GMF has convened an expert-led Global Task Force for the Trusted Sharing of Data that is working on a roadmap to enable data flows with enforceable human rights protections.

Cybersecurity

Rising global awareness of cyber threats has coincided with an increase of cyber alliance-like ties among democratic nations, including a commitment to apply NATO's Article 5 joint defense provision in the event of a serious cyberattack.

The Biden administration collaborated actively on cyber defense for Ukraine and Western allies in the buildup to Russia's invasion of Ukraine. The cooperation created mechanisms for sharing actionable cyber threat intelligence with allies and with the US private sector. Washington boosted capacity-building programs to provide expertise and support for allies' responding to cyber incidents and now exchanges cybersecurity good practices with those partners. All this occurred before the confirmation of a State Department cyber ambassador, who will work to deepen the collaboration.

The clearest result of these efforts is the Counter Ransomware Initiative, an alliance of 13 companies and 37 countries that have pledged to confront the threat of ransomware. The scope of the initiative is broad, including cooperation on criminal prosecutions, asset seizures, crackdowns on cryptocurrency exchanges, and defend-forward, preemptive cyberattacks against threatening actors.

Rising global awareness of cyber threats has coincided with an increase of cyber alliance-like ties among democratic nations, including a commitment to apply NATO's Article 5 joint defense provision in the event of a serious cyberattack.

The Biden administration is also taking action on its own. The White House released an executive order to restrict hostile intelligence agencies from gaining access to data—on servers, submarine cables, and other points of access—about US persons, and it is working on further measures to curb this risk. The Department of Commerce published a list of Chinese and Russian companies with military ties for inclusion in a list of entities to exclude from US supply chains on national security grounds. The department's move followed the Trump administration's executive order on keeping information and communications technology and services supply chains from adversaries. Efforts to exclude their state-owned companies from the US market also got a legal boost when, in January 2023, a circuit court issued a broad ruling upholding the revocation of China Telecom's authorization to provide services in the United States. The court made clear that national security exclusion orders have priority and that no evidence of a cyber incident involving an entity is required to revoke its ability to operate in the United States.

The White House also continues to evaluate a strategy for TikTok, the popular video sharing app. A Trump administration executive order effectively banning that platform and WeChat by prohibiting their downloads or security updates from US app stores was ultimately unsuccessful. The order failed because it leap-frogged a Department of Commerce investigation that provided only scant evidence substantiating security concerns. The order also neglected to address statutory restrictions on applying export controls to First Amendment-protected speech. The Biden administration responded with its own executive order that gave the department more specific instructions. In addition, the Committee on Foreign Investment in the United States, which scrutinizes national security implications, is reviewing TikTok and considering, press reports say, requiring the platform to separate itself from its Chinese parent company, ByteDance, or to restructure. Congress passed its own measure last year barring use of TikTok on US government computers and a significant number of US states have followed suit. A bipartisan

group of Senate and House lawmakers, led by Senator Marco Rubio, has also signed onto a bill that would ban TikTok from operating throughout the United States. TikTok has responded by attempting to forge an agreement under which data on users in the United States would be held by a domestic third party and be inaccessible from China.

Information Integrity

The United States lacks a strategic framework for analyzing and addressing information operations or information warfare, which the Congressional Research Service says is regularly defined as "a strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations". The absence of a strategy is in part due to the sensitive nature of safeguarding online freedom of expression. Also, many definitions are used across government agencies to describe information operations—including those for hybrid threats, hack and leak, and strategic disinformation. The press and public, meanwhile, discuss misinformation and disinformation, which misleadingly suggests that the problem is merely determining what is true and what is false. A strategic framework would clarify policy options and provide grounding for law enforcement and the intelligence community to separate First Amendment-protected speech from illegal activity.

The EU faces similar challenges but is attempting to address the spread of illegal content through its Digital Services Act (DSA) and the concentration of power through its Digital Markets Act (DMA). Although these reflect a different legal context from that in the United States, there is room for transatlantic cooperation on the DSA requirement for platform risk assessments and for platforms to share data with researchers.

An ongoing commitment to an independent press can also bolster information integrity. Some democracies have supported international independent journalism since World War II and continue to do so. Congress has increased funding for outlets such as Radio Free Europe/Radio Liberty and Radio Free Asia, and for protecting independent journalists targeted for their work. Western allies also coordinate responses to authoritarian state information operations through initiatives such as NATO's Strategic Communications Centre of Excellence and the State Department's Global Engagement Center.

Censorship Circumvention and Protection From State Surveillance

The United States continues to work to protect individuals' ability to circumvent censorship and internet shutdowns even as authoritarian regimes grow ever more sophisticated in their ability to deny access and engage in digital surveillance and control. Washington has increased funding for the Open Technology Fund, which provides virtual private networks (VPNs) and other tools to help people living under repressive regimes access the internet and avoid surveillance. The Treasury Department has exempted from Russian sanctions "the exportation or reexportation, sale, or supply, directly or indirectly, from the United States or by [US] persons, wherever located, to the Russian Federation of services, software, hardware, or technology incident to the exchange of communications over the internet". The same humanitarian exemption applies to Iran and Syria.

Defending digital democracy should build on the new, White House-championed Declaration for the Future of the Internet, a commitment signed by 61 countries promising to uphold an "open, free, global, interoperable, reliable, and secure Internet". Its principles include protection of fundamental freedoms, free flow of information, the right to connectivity, privacy protection, and a commitment to a multistakeholder internet-governance approach. It condemns authoritarian digital measures such as repression of free expression, censorship, and the fracturing of the global internet ("splinternet"). The declaration can be a promotional vehicle in multistakeholder and multilateral forums, and the State Department's new Cyber Bureau could spearhead the effort. But policy development is needed as well. This includes:

Preparing for new cybersecurity challenges and developing standards: Increased challenges and opportunities posed by new technologies must be addressed. These include the threat of faster quantum computing to encryption; the development

of the Internet of Things; and the proliferation of space servers. A study of lessons learned from Russia's use of cyberattacks in its invasion of Ukraine, and the Western response to those attacks, can help inform strategy. Efforts to develop, with US allies, interoperable cybersecurity procurement standards and to block China's efforts to promote standards favorable to its vulnerable technology, are already underway.

Information integrity strategy: A strategic framework is needed to distinguish among foreign state action requiring attribution, removal, and correction (e.g., the Russian information operations that accompanied a financial cyberattack on Ukraine); illegal actions requiring law enforcement action against individuals (e.g., incitement, targeted harassment, voter suppression, campaign finance violations, and civil rights violations); and information pollution requiring longer-term action to promote social resilience through media literacy, greater transparency, support for independent journalism, and a "PBS of the internet" civic information effort.

Multistakeholder efforts to combat state censorship, shutdowns, and surveillance: The United States has committed to chair the Freedom Online Coalition starting in 2023. This and the Declaration for the Future of the Internet can be powerful vehicles for the new State Department Bureau for Cyberspace and Digital Policy and for White House officials to work with civil society, technologists, and industry.

CONCLUSION

A new US foreign policy of technology can successfully support innovation-led leadership but only by engaging in diplomacy and with stakeholders. This is possible by creating new multistakeholder institutions that would plug the current global economic system's gaps. These combined initiatives would construct a new architecture comprising:

- A **Digital Policy Lab** to nurture innovation. The lab would build capacity for implementing new initiatives; coordinate funding priorities, reporting, and communication; serve as a data repository; and provide accountability.
- A **Technology Task Force** to coordinate efforts to safeguard sustainable, secure supply chains. This multistakeholder body's responsibilities should include information-sharing, targeted subsidies, and R&D coordination. It should begin by focusing on semiconductors and clean technology supply chains.
- The **Declaration for the Future of the Internet** and a campaign to promote and strengthen it. This would renew the commitment to internet freedom while guarding against cybersecurity risks, strengthening an information integrity strategy, and combatting state-sponsored shutdowns, censorship, and surveillance.

Significant progress has been made in responding to interconnected technology challenges, whether they concern semiconductors, supply chains, or sanctions. This in itself is a recognition that post-Cold War assumptions and institutions require an update for 21st-century foreign and economic policy.

The additional steps outlined above ensure that a new approach remains durable, flexible, and tied to the core values of the United States and its allies.

The views expressed in GMF publications and commentary are the views of the author(s) alone.

As a non-partisan and independent research institution, The German Marshall Fund of the United States is committed to research integrity and transparency.

About the Author(s)

Karen Kornbluh is the managing director of GMF's Digital Innovation and Democracy Initiative.

Julia Tréhu is a program manager and fellow with GMF's Digital Innovation and Democracy Initiative.

About GMF Digital

The German Marshall Fund's Digital Innovation and Democracy Initiative (GMF Digital) works to support democracy in the digital age. GMF Digital leverages a transatlantic network of senior fellows to develop and advance strategic reforms that foster innovation, create opportunity, and advance an equitable society.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of the Second World War, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

Cover photo credit: metamorworks | Shutterstock