

# Agile Alliances

HOW THE UNITED STATES  
AND ITS ALLIES CAN  
DELIVER A DEMOCRATIC  
WAY OF AI

AUTHORS

Andrew Imbrie  
Ryan Fedasiuk  
Catherine Aiken  
Tarun Chhabra  
Husanjot Chahal





## CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

Established in January 2019, the Center for Security and Emerging Technology (CSET) at Georgetown's Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. CSET aims to prepare a generation of policymakers, analysts, and diplomats to address the challenges and opportunities of emerging technologies. During its first two years, CSET will focus on the effects of progress in artificial intelligence and advanced computing.

[CSET.GEORGETOWN.EDU](https://CSET.GEORGETOWN.EDU) | [CSET@GEORGETOWN.EDU](mailto:CSET@GEORGETOWN.EDU)

---

# Agile Alliances

HOW THE UNITED STATES AND ITS ALLIES  
CAN DELIVER A DEMOCRATIC WAY OF AI



## AUTHORS

Andrew Imbrie  
Ryan Fedasiuk  
Catherine Aiken  
Tarun Chhabra  
Husanjot Chahal

## ACKNOWLEDGEMENTS

This report is about how to strengthen U.S. alliances and partnerships in AI. In the process of researching and writing, the authors benefited from the insights of many allies of their own. Thanks to Jason Matheny, Igor Mikolic-Torreira, Dewey Murdick, Helen Toner, and Lynne Weil for critical support and valuable comments. Huey-meei Chang, Teddy Collins, Melissa Flagg, Roxanne Heston, Saif Khan, William Hannas, Michael Page, and Remco Zwetsloot provided excellent feedback and suggestions. Thanks also to Matt Mahoney, Maura McCarthy, and Alexandra Vreeman for editorial support.

We are grateful to Ulrike Franke of the European Council on Foreign Relations and Jim Townsend of the Center for a New American Security for reviewing the report and offering crucial insights and perspective. Thanks to Tim Rudner and Jack Clark for their comments on the survey methodology. For help with the coding of the national AI strategies, we are grateful to student researchers Kady Arthur and Bianca Campos-Scheibel. Special thanks to Kady for her diligence in compiling Appendix III. The authors are solely responsible for the opinions, conclusions, and policy recommendations contained in this report.

© 2020 Center for Security and Emerging Technology,  
All rights reserved.

Cover photo: Adobe Stock/This is brk.

Document Identifier: doi: 10.51593/20190037

# Contents

---

EXECUTIVE SUMMARY: FORGING A DEMOCRATIC WAY OF AI	iii
INTRODUCTION	ix
1   AMERICA’S ENDURING ADVANTAGE: TRUST AND TRADE-OFFS	1
2   METHODOLOGY	5
3   UNDERSTANDING COLLABORATIVE PARTNERS	7
4   STRATEGIC INITIATIVES	11
CONCLUSION	39
APPENDIX I. SURVEY METHODOLOGY	41
APPENDIX II. METHODOLOGY FOR ASSESSING TECHNOLOGY TRANSFER VECTORS AND VULNERABILITIES	43
APPENDIX III. MULTILATERAL FORA FOR AI COOPERATION	45
ENDNOTES	55



# Executive Summary

## Forging a Democratic Way of AI

**H**ow can the United States collaborate with allies and partners to shape the trajectory of artificial intelligence in ways that will promote liberal democratic values and protect against efforts to wield AI for authoritarian ends?

This question is both important and urgent. It is important because America's broad network of alliances and security partnerships is a singular asset in defending liberal values. It is urgent because China, Russia, and other authoritarian powers seek to achieve strategic advantage through AI and the export of censorship and surveillance technologies to countries across the globe.<sup>1</sup> By one estimate, more than 100 countries purchase surveillance and censorship gear from China and Russia, receive training on these technologies, or simply imitate methods of surveillance and censorship that are designed to control public opinion and stifle dissent.<sup>2</sup>

As the digital and physical environments become intertwined, authoritarian practices in one domain will increasingly encroach upon the other. At stake are the core values of liberty, equality, and justice that underpin free and open societies. All democratic nations must work together to uphold basic principles, set international rules of the road, and articulate a positive vision for the future in the age of AI.

Within the United States, and certainly within allied countries, debate persists over the threat of digital authoritarianism and how to counter it. While U.S. allies will likely vary in their strategic orientations toward China and Russia, there is a growing consensus on the need to showcase a democratic way of AI. These debates will take shape in a world of globalized

markets for AI talent and integrated supply chains. In this context, the right U.S. approach would leverage its network of allies and partners to safeguard democracy and liberal values. An alliance-centric strategy provides a competitive advantage over any single country that attempts to develop a robust AI ecosystem on its own.

The United States and its allies should play to their strengths. This positive agenda begins with shaping the ecosystems for the development and deployment of safe and reliable AI. The most effective approach would capitalize on advances in AI and machine learning to foster sustainable and inclusive economic growth, improve service delivery, and promote transparent and accountable governance. The United States and its allies should pursue a vision of the future in which AI enables strengthened data privacy standards and respect for civil liberties; economic empowerment of citizens within rules-based market economies; cleaner, safer, and more efficient transportation; precision medical diagnosis; greater access to education; and more effective disaster response.

This report presents novel, if preliminary, data to make the case that the United States can work with like-minded allies and partners to forge a democratic way of AI.<sup>3</sup> It offers the first comprehensive analysis of how the United States can cooperate with allies and partners in AI by drawing on several original data sets, including a cross-national survey of official government representatives, a unique coding of national AI strategies, and a comparative assessment of Chinese professional and technology associations in U.S. allied and partner countries. To supplement these measures, we aggregate data from multiple sources to assess U.S. allies and partners according to their *capability* and *compatibility* in AI and machine learning.<sup>4</sup>

Based on this analysis, the report proposes 10 strategic initiatives for the United States to pursue with its allies and partners. It identifies the optimal partners on each initiative and highlights existing multilateral channels for engagement. A unifying appeal to shared values would not only safeguard those values, but also advance AI research and development, protect supply chains and sensitive technologies, and promote collaboration among U.S. allies and partners on critical security and economic priorities.

The United States and its allies should pursue a three-pronged strategy: (a) **defend** against the threats posed by digital authoritarianism, (b) **network** with like-minded countries to pool resources and accelerate technological progress, and (c) **project** influence and leverage safe and reliable AI in support of inclusive growth, human rights, and liberal democratic values.



To that end, we recommend the following 10 initiatives:

## DEFEND

- **Initiative 1: Prevent the transfer of sensitive technical information.** U.S. counterintelligence, law enforcement, and other relevant government officials should coordinate with their counterparts in allied countries to gather and analyze data on technology transfers at scale, standardize visa screening procedures, and develop shared standards and metrics to evaluate transactions over the short, medium, and long term.

*Optimal Partners:* Germany, the United Kingdom, Japan, Canada, France, and Australia

*Multilateral Fora:* European Union, North Atlantic Treaty Organization, Multilateral Action on Sensitive Technologies conference, Office of the Director of National Intelligence- and Federal Bureau of Investigation-led multilateral dialogues with counterintelligence and law enforcement officials of allied and partner countries

- **Initiative 2: Coordinate investment screening procedures.** The United States and its allies should coordinate investment screening procedures, clarify the transactions posing a national security risk to U.S. and allied supply chains, and establish data-driven criteria for assessing risk.

*Optimal Partners:* The United Kingdom, Germany, the Netherlands, France, Italy, and Japan

*Multilateral Fora:* European Union, Joint Committee on Foreign Investment in the United States-European Union screening dialogues, Group of Seven, Office of the Director of National Intelligence- and Federal Bureau of Investigation-led multilateral dialogues with counterintelligence and law enforcement officials of allied and partner countries

- **Initiative 3: Exploit hardware chokepoints.** The United States should coordinate with allies and partners on export controls targeting components of the supply chain that increase the probability of maintaining China's dependence on imports of AI chips.

*Optimal Partners:* Taiwan, South Korea, Japan, Israel, Singapore, and the Netherlands

*Multilateral Fora:* SEMI (Semiconductor Equipment and Materials International), World Semiconductor Council, U.S.-South Korea-Japan Trilateral Strategic Dialogue, Group of Seven, Wassenaar Arrangement

## NETWORK

- **Initiative 4: Share, pool, and store non-sensitive datasets.** The United States should work with allied and partner governments to develop common standards for sharing, pooling, and storing non-sensitive, government-owned datasets, including datasets related to weather patterns, epidemiological data for disease control, video and navigation data from self-driving cars, and relevant data for predictive maintenance and maritime domain awareness.

*Optimal Partners:* The United Kingdom, Germany, Japan, France, the Netherlands, and New Zealand

*Multilateral Fora:* North Atlantic Treaty Organization, the European Commission, Five-Eyes, Organization for Economic Cooperation and Development, and the Association of Southeast Asian Nations

- **Initiative 5: Invest in privacy-preserving machine learning.** To protect individual privacy, the United States and its allies and partners should explore techniques in data analysis that would allow them to perform operations on non-sensitive datasets without sharing or storing personally identifiable information.

*Optimal Partners:* Canada, India, Germany, Australia, Japan, and the United Kingdom

*Multilateral Fora:* European Union, Organization for Economic Cooperation and Development, the Quadrilateral Security Dialogue (India, Japan, Australia, and the United States); National Institute of Standards and Technology- and National Science Foundation-led bilateral and multilateral partnerships

- **Initiative 6: Promote interoperability and agile software development.** As countries integrate AI into military systems, the United States and its allies must ensure that hardware and digital systems are interoperable and secure, beginning with common standards for interpretability, safety, and security of AI systems, including AI-enabled, safety-critical systems.

*Optimal Partners:* Canada, Australia, the United Kingdom, Germany, Italy, and Japan

*Multilateral Fora:* Five Eyes, North Atlantic Treaty Organization, North Atlantic Treaty Organization-European Union (AI4EU) test bed partnership, U.S.-Japan-South Korea Trilateral Defense Cooperation, National Technology and Industrial Base (Australia, Canada, the United Kingdom, and the United States)

- **Initiative 7: Launch an AI R&D collaboration challenge.** U.S. and allied science funding organizations should expand coordination to solicit research on complementary agendas, such as human-machine teaming methods, autonomous vehicles, and verification techniques for complex control systems and AI-enabled, safety-critical infrastructure.

*Optimal Partners:* Japan, Germany, South Korea, France, the United Kingdom, and the Netherlands

*Multilateral Fora:* European Union, Multilateral Action on Sensitive Technologies conference, Organization for Economic Cooperation and Development, Association of Southeast Asian Nations, National Science Foundation-, National Institutes of Health-, and Department of Energy-led innovation dialogues

- **Initiative 8: Develop inter-allied human capital for AI.** The United States should facilitate the exchange of knowledge and best practices on AI among allied and partner countries by convening workshops among AI researchers, fostering international networks of AI researchers, and deepening partnerships with existing networks, including coordination with the private sector on job placement and training programs.

*Optimal partners:* India, the United Kingdom, Germany, France, Canada, and South Korea

*Multilateral Fora:* European Union, Institute of Electrical and Electronics Engineers, exchange programs modeled on CRDF Global and the United States Telecommunication Training Institute, National Science Foundation international partnerships

## PROJECT

- **Initiative 9: Shape global norms and standards for AI.** Building on the Organization for Economic Cooperation and Development Principles on AI, the United States should lead a multilateral effort with allies and partners to set international rules of conduct for AI, including standards for testing, evaluation, verification, and validation of AI technologies, as well as common practices for certifying companies that support democratic values and privacy.

*Optimal Partners:* Canada, the United Kingdom, Ireland, Australia, Singapore, and Japan

*Multilateral Fora:* European Union, Organization for Economic Cooperation and Development, International Organization for Standardization, International Organization for Standardization and International Electrotechnical Commission Joint Technical Committee 1 Sub Committee 42 – Artificial Intelligence, World Trade Organization, 3rd Generation Partnership Project, North Atlantic Treaty Organization-European Union joint initiative on standards for emerging technologies

- **Initiative 10: Establish a multilateral digital infrastructure network.** The United States and its allies should launch a multilateral digital infrastructure network to ensure that digital systems in emerging markets are open, secure, resilient, and interoperable, while empowering developing countries to protect data privacy, meet their domestic needs, and access high-performance computing and mobile internet technologies.

*Optimal Partners:* Germany, Japan, France, the United Kingdom, Ireland, and Canada

*Multilateral Fora:* European Union, International Monetary Fund, World Bank, European Bank for Reconstruction and Development, Asian Development Bank, Digital Nations (The Digital 9)

# Introduction

**T**he United States has long benefited from its network of allies and partners that contribute forces, specialized capabilities, and legitimacy to U.S. leadership in the world. In recent years, however, this network has come under strain. Disputes over burden sharing and mutual recriminations have raised questions about the cohesion and durability of existing alliance structures. Recent U.S. policy shifts and withdrawal from certain international agreements have deepened fears that the United States no longer sees its allies and partners as central to U.S. strategic objectives and national security.

America's alliances are weakening at a time of growing competition between democratic nations and authoritarian regimes. Authoritarian regimes are surviving longer and becoming more adept at using AI-enabled surveillance and censorship technologies to export their values abroad.<sup>5</sup> China and Russia present a significant challenge to liberal democratic societies.<sup>6</sup> A world in which China and Russia deploy AI to widen the net of information controls is a world of diminished rights and protections for the individual, fewer safeguards for privacy and the rule of law, more data exploitation, and limited opportunities for judicial redress or public dissent.<sup>7</sup>

Despite the importance of alliances in promoting democratic values and protecting against a mounting authoritarian challenge, the United States lacks a strategic approach for cooperating with allies and other like-minded partners on AI.

This report assesses where collaboration on AI with allies and partners can advance U.S. and allied interests and values. It begins by analyzing the trade-offs that U.S. and allied policymakers will need to manage in order to bolster cooperation in AI. Next, it specifies the methodology,

including scope, case selection, survey design, and data collection. The report then outlines 10 strategic initiatives for the United States to pursue with its allies and partners. After identifying promising areas of cooperation, the report highlights which actors would make the most strategic partners for each initiative. In comparing allies, we include indicators that reflect both the AI-relevant capability they bring to the table in terms of data, algorithms, talent, and computing power, and the compatibility of their interests and values with those of the United States.

# 1 America's Enduring Advantage

## Trust and Trade-offs

**A**merica's broad network of allies and partners is a source of enduring strength. In an era of economic and technological competition with China and Russia, the United States benefits from allies that share its values and produce troves of strategic resources, including computer and data science experts; private sectors that are innovative, dominant and trend-setting; data on which to train AI algorithms; advanced microprocessors and data storage units; governmental research and development (R&D) investments; diplomatic support for initiatives in AI safety and governance; and the clout needed to export norms and best practices to the rest of the world.

Alliances matter in the AI context because they provide a framework for cooperation, data sharing, dissemination of best practices, joint planning, and procurement. The market adequately incentivizes some forms of cooperation, such as data labelling and exchanges. But alliances can help formalize and expand these relationships, correct for market failures in such areas as AI safety and security, coordinate development of use cases and risk assessments, enhance the legitimacy of international action, and validate the deployment of safe and reliable AI.

America's alliances and security partnerships will shape the future trajectory of AI, even as AI reshapes the capabilities and operating environments for U.S. allies and partners. By investing in privacy-preserving machine learning and other techniques for improving the interpretability of AI systems, the United States and its allies can promote the development of AI consistent with liberal democratic values. Far-sighted investments could yield large dividends. AI has a wide array of applications that can benefit

democracies, from improving data protection and privacy, to promoting transparency and accountability in government.

Advances in AI will also enable new military capabilities. Nations around the world use AI to enhance intelligence collection and analysis, streamline decision-making, lower operating costs, and improve military logistics through predictive maintenance. As China, Russia, and other authoritarian powers integrate AI with military capabilities, U.S. allies and partners will face a more complex operating environment. Advances in software and digital systems could render it more difficult to assess the balance of power in key domains. As the operational tempo of war accelerates, leaders might be tempted to integrate AI and machine learning into early warning and command and control systems, creating new risks and uncertainties for strategic stability.<sup>8</sup> Competitors may rush to deploy AI-enabled capabilities without adequate testing, evaluation, verification, and validation. Compounding the risks, adversaries will seek to exploit vulnerabilities in AI systems and may even use AI to execute novel cyberattacks and disinformation campaigns aimed at undermining democratic institutions and sowing discord among the public.<sup>9</sup>

In meeting these challenges and seizing the opportunities that AI presents, the United States and its allies face tough trade-offs. Three, in particular, necessitate close coordination and prudent mitigation strategies.

First, the United States and its allies face a trade-off between **capability and dependency**.<sup>10</sup> Showcasing a democratic way of AI will require the United States and its allies to pool resources, coordinate policies, and share best practices and information. Leveraging the capabilities of its allies and partners will amplify U.S. power and influence, but will also create inefficiencies and require compromise. While the United States can manage these challenges, it cannot eliminate them entirely—nor should it. As long as AI-related supply chains are global and AI talent both mobile and globally distributed, innovation in AI requires international collaboration.<sup>11</sup> To excel in this new context, America will need to embrace its role as a “systems integrator” among like-minded allies and partners.<sup>12</sup> Embedding cooperation in dense, decentralized networks plays to the United States’ strengths as a democratic power that favors market approaches to technological cooperation. By combining top-down vision with dynamic, bottom-up innovation and entrepreneurship, the United States and its allies can foster a competitive ecosystem that enables the best ideas to flourish.

These benefits should not obscure the risks. International networks can facilitate cooperation by creating focal points and enhancing the transparency and availability of information.<sup>13</sup> As scholars have shown, however, networks of interdependence can also become the sites of competitive power plays, such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) financial messaging



system.<sup>14</sup> The United States has used SWIFT to counter terrorism, monitor illicit financial activity, and bolster the sanctions regime against Iran.<sup>15</sup> At the same time, China is exploring alternatives to this U.S.-dominated cross-border payments system.<sup>16</sup> Emerging competitive dynamics suggest the need for a strategic approach toward the development of AI, especially in semiconductors.

To manage the risks, the United States and its allies should pursue a range of mitigation strategies, including securing and enhancing their defense innovation bases and domestic economic competitiveness, diversifying partnerships in AI, investing diplomatic capacity in norms and standards for AI technologies and mobile telecommunications consistent with democratic values, and promoting flexible institutional configurations for partnership in AI.<sup>17</sup>

Second, the United States and its allies face a trade-off between **competition and cooperation**. All nations compete for relative military and economic advantage. In the age of AI, nations will also compete over whose vision of the future attracts the broadest support. Cooperation among democracies is necessary to guard against authoritarian uses of AI, but there are other imperatives for cooperative action. For example, democratic nations must cooperate with strategic competitors to ensure global economic stability and prevent misperceptions and miscalculations from spiraling into hostility; this could be achieved through arms control or international action to create norms and standards for emerging technologies.

Conventional wisdom suggests that the United States competes with China and Russia in AI and collaborates with allies and partners. While accurate, it is equally true that the United States competes with its allies and partners for top talent and resources in AI and must find ways to cooperate with China and Russia on AI safety and security, strategic stability, and crisis management to forestall the risks of accidents and miscalculations.<sup>18</sup> When asked about obstacles to collaboration with the United States, for example, multiple officials from allied countries highlighted industrial competition as an impediment.

Cooperative dynamics are typically in pursuit of shared, global interests, while competitive dynamics tend to follow from a national calculation of AI's impact on relative power and wealth. Researchers and scientists cooperate across national boundaries, but political leaders face difficult trade-offs between national interests and the international networks that foster open-source collaboration in AI.

Navigating these dynamics will require the United States and its allies to pursue a two-pronged strategy: expand areas for cooperation and competition that generate mutual benefits, while shrinking the space for competition that generates harmful effects or a race to the bottom. For example, the United States should manage competition within a rules-based framework that ensures a level playing field, protects intellectual property, and disincentivizes hidden government subsidies. At

the same time, it should work with countries to discourage unfair competition that tilts the playing field in favor of state-backed enterprises, destabilizes financial markets, and triggers unforeseen disruptions to global supply chains.

The third trade-off is between **safety and speed**.<sup>19</sup> This trade-off arises from the complex dynamics between the United States and its allies on the one hand, and strategic competitors such as China and Russia on the other. Artificial intelligence presents a range of opportunities and risks for the United States and its allies. AI systems are brittle and can fail accidentally or behave unpredictably in real-world settings.<sup>20</sup> American, European, Chinese, and Russian leaders increasingly view AI as a core element of national power. In an effort to gain comparative advantage, countries could rush to deploy untested or unsafe AI systems. It is in the interest of U.S. national security to pursue confidence-building measures in AI safety. It is also a core interest of U.S. allies: a majority of officials noted standards to ensure reliable and responsible AI development as a national AI priority and avenue for productive multilateral collaboration. By leading an international effort on safe and reliable AI, the United States and its allies can reduce threats to global security and promote strategic stability.

Policymakers could pursue any number of initiatives in this area, such as bringing together technical experts from the United States, China, and Europe to define shared concepts and standards for the robustness of AI systems; pursuing low-stakes joint projects to summarize the AI safety literature in different countries and promote transparency into applications of AI safety research; facilitating Track 1.5 and Track 2 dialogues on specific challenges in AI safety; or developing common standards and methods of testing, verifying, and validating AI systems, including AI-enabled safety critical infrastructure.<sup>21</sup>

## 2 Methodology

Several reports have analyzed comparative national strategies in AI.<sup>22</sup> Others have scored countries in terms of “AI readiness” and “AI performance.”<sup>23</sup> For example, the BSA Global Cloud Computing Scorecard rates countries according to data privacy, security laws and regulations, cybercrime and intellectual property rights.<sup>24</sup> Benchmarks from the Capgemini consulting group, McKinsey, and PricewaterhouseCoopers are important for cross-national comparisons, but they do not examine AI in the context of alliances or consider how the United States can best leverage its existing alliances and security partnerships for the development and deployment of safe, reliable AI.

*Scoping Policy Options:* This paper is premised on the idea that the United States should work with different sets of allies and partners to accomplish different AI-relevant policy goals. It groups policy options into 10 strategic initiatives. We formulated these options by talking with policymakers in the United States and in allied and partner nations, canvassing the literature about emerging threats and opportunities, and formally surveying foreign diplomats and government stakeholders.

*Selecting Cases:* For each initiative, we identified the optimal cluster of allies and partners. The population of cases is based on two criteria: countries must a) participate in a mutual defense treaty, strategic partnership, or cooperative defense agreement with the United States, and b) have developed or announced a plan to develop a national AI strategy.<sup>25</sup> Using these two criteria, our final case list comprises 38 countries and jurisdictions.<sup>26</sup>

*Surveying Partners:* To better understand the AI-relevant priorities of allies, we surveyed official representatives of 27 countries from our final case list, plus the European Union (EU).<sup>27</sup> Fifteen government officials from


11 countries and the EU completed the survey. While fifteen is a modest number of survey respondents, the individual responses provided a wealth of insights into the AI priorities, evolving AI strategies, and level of interest in international collaboration around AI among allies and partners.

*Evaluating Partners:* Within the context of a specific policy initiative, we measure each country's capability in terms of technological, economic, and social resources, as well as its compatibility with U.S. interests, values, and policy goals.

Using publicly available datasets, commercially available reports, and survey data, we selected or created 84 metrics. Each indicator is relevant to at least one of the policy initiatives outlined. We group the indicators by relevance, using between 5 and 15 metrics to highlight the most capable and compatible countries for each initiative. The weighting ascribed to metrics for capability and compatibility varies by initiative.

Not all indicators are equally relevant, and each metric highlights unique strengths. To prevent technology transfer, for example, policymakers may assign varying degrees of importance to the number of Chinese students in a country or the number of journal articles scientists in that country have produced. For each initiative, we list "optimal countries" (highest average composite scores of indicators). We provide the raw metrics in a table for the top six U.S. allies and partners so that readers can judge for themselves which values are most important to crafting a democratic way of AI.

### 3 Understanding Collaborative Partners

 Our cross-national survey of government officials asked questions about national AI R&D priorities, international coordination and data sharing preferences, AI talent development strategies, and perceptions of other countries' approaches to AI. Table 1 outlines the findings on national AI priorities. Officials cited four primary areas of concern around AI: domestic social and economic issues, domestic security, international security, and ethics. Domestic economic and social issues were the most prevalent area of concern, primarily labor market impacts and privacy. In terms of optimism, almost all officials focused on AI's potential to advance domestic industry, services, and governance. Benefits for health, education, and infrastructure were especially prevalent.

National R&D priorities focus on increasing research coordination and capabilities and boosting domestic industry. Priorities to advance capabilities included increasing investment, fostering technical innovation, establishing AI centers, developing international research initiatives, and training AI talent. Allies and partners prioritize AI R&D investments that support domestic ecosystems, with a focus on improving health, education, transportation, and public goods provision. AI R&D priorities are not determined solely by government actors; industry actors play an important role in the process, as well. Officials noted multiple channels for industry consultation and stressed that the voice of the private sector is important in shaping national AI strategies. Some officials highlighted that industry takes the lead in determining R&D priorities, with government backing and support. A few officials noted that national R&D priorities are still in flux, indicating room for U.S. leadership on this front.

TABLE 1

## AI Priorities of Partner Countries

AI APPLICATIONS OF CONCERN	AI APPLICATIONS OF OPTIMISM	NATIONAL AI R&D PRIORITIES
<b>Domestic Economy &amp; Society (10)</b>	<b>Domestic Services &amp; Governance (13)</b>	<b>Research &amp; Technological Capabilities (9)</b>
<ul style="list-style-type: none"> <li>• Labor disruption</li> <li>• Discrimination &amp; bias</li> <li>• Industrial competition</li> <li>• Privacy</li> <li>• Disinformation</li> </ul>	<ul style="list-style-type: none"> <li>• Health &amp; medicine</li> <li>• Government logistics</li> <li>• Productivity</li> <li>• Education</li> <li>• Infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>• Basic research</li> <li>• Investment</li> <li>• AI labs</li> <li>• Training talent</li> <li>• Computing power</li> </ul>
<b>International Security (7)</b>	<b>International Development (4)</b>	<b>Domestic Services (8)</b>
<ul style="list-style-type: none"> <li>• Human rights</li> <li>• Lethal autonomous weapons</li> <li>• Malicious actors</li> </ul>	<ul style="list-style-type: none"> <li>• Sustainable Development Goals</li> <li>• Climate change</li> <li>• Disaster prediction</li> </ul>	<ul style="list-style-type: none"> <li>• Transportation</li> <li>• Health</li> <li>• Education</li> <li>• Business</li> </ul>
<b>Domestic Security (5)</b>		<b>AI Ethics (4)</b>
<ul style="list-style-type: none"> <li>• Law enforcement</li> <li>• Cyberattacks</li> <li>• Surveillance</li> </ul>		<ul style="list-style-type: none"> <li>• Reliable AI</li> <li>• Alignment with democratic values</li> </ul>
<b>AI Ethics (4)</b>		
<ul style="list-style-type: none"> <li>• Legal &amp; ethical gaps</li> <li>• Lack of transparency</li> </ul>		

Note: Numbers in parentheses signify the number of representatives who indicated a priority in that category.

Source: CSET Survey

All surveyed officials indicated that they engage with international partners on AI-related issues. Bilateral efforts were the most cited avenue of international collaboration on AI, in four cases (EU, Australia, Czech Republic, and Italy) involving the United States. Multilateral fora were another common and increasingly relevant avenue for collaboration. The Organization for Economic Cooperation and Development (OECD) was the most cited multilateral forum, while multiple officials indicated engagement through the EU, Group of Seven (G7), Group of Twenty, or the newly created Global Partnership on AI (GPAI). Current international efforts focus on developing shared ethical standards, in part following the lead of the OECD and

EU on defining AI standards. Other officials noted collaboration around workforce challenges, data policies, climate change, and lethal autonomous weapons systems (LAWS).

Partners' active engagement and interest in international collaboration around AI is matched with positive perceptions of the United States' role as an AI partner. Eighty percent of officials said their country considers the United States to be a reliable partner on AI issues. The remaining three officials, representing the EU, Germany, and France, suggested that while they consider the United States a like-minded ally and continue to value U.S. partnership, recent exchanges have been less fruitful and current approaches raise general concerns regarding U.S. reliability as an AI partner. Officials also rated the United States highly in terms of commitment to responsible use of AI with an average rating similar to the average rating of their own countries, or institutions, in the case of the EU, and a significantly higher rating than they assigned to China's commitment to responsible AI (7.3, 7.9, and 3.8 out of 10, respectively).

In citing obstacles to collaboration with the United States, officials were split between placing blame on the United States and on their own country. Multiple officials noted threats to industry and industrial competition, trade issues, different domestic priorities, or a lack of agreed upon strategy or common structures as obstacles to collaboration. Others specified that the U.S. desire to "win" relative to China, lack of data privacy protection, or unwillingness to engage inhibited collaboration. They also noted a lack of confidence in current U.S. goals or appropriate U.S. points of contact. Obstacles stemming from their own government included a lack of regulatory framework or set policies, alternative political priorities, a preference for multilateral fora, or insufficient resources.

The survey results indicate that there is space for the United States to engage with international partners and, despite some specific but not insurmountable points of difference, a high degree of alignment on AI interests and priorities.





## 4 Strategic Initiatives

**T**he following 10 initiatives provide a roadmap for how the United States and its allies can defend against threats, network to seize opportunities, and project influence to safeguard democracy in the age of AI.

### DEFEND AGAINST THREATS

#### **Initiative 1: Prevent the transfer of sensitive technical information.**

The Chinese government undertakes multiple, coordinated efforts to obtain sensitive information from U.S. AI researchers. Many of these pathways and access points for technology transfer are legal or extra-legal and therefore poorly understood or monitored by Western intelligence agencies.<sup>28</sup> Common vectors include technology transfer centers and forums, copyright infringement, and grant and funding opportunities for Chinese undergraduate, graduate, and post-doctoral researchers to study abroad and collaborate with foreign universities, research labs, and companies.<sup>29</sup>

International partners share U.S. concerns about the transfer of sensitive technology: just over half of survey respondents indicated that their government has concerns about foreign talent studying or working in fields with military or national security applications, and a majority of officials (60 percent) stated that their governments have policies in place to counter the transfer of sensitive technologies.<sup>30</sup> A third of respondents did not know if their governments shared such concerns, indicating an opportunity for U.S. leadership on this issue.

The United States could improve coordination with allies and partners to counter technology transfer in several ways. Officials from each sur-

veyed country indicated interest in coordinating with the United States to prevent the transfer of sensitive technology. This initiative received the second highest level of agreement, just after coordinated AI norms and standards. Respondents from Japan, Australia, Italy, and France were particularly interested in collaboration around tech transfer policies.

The United States should work with its allies and partners to build an empirical base of knowledge on this issue, supported by robust data collection and analysis. Survey results suggest that allies believe international management is required to counter cyber exploitation, with nearly 75 percent of officials noting it as a trend requiring international coordination. By launching a multilateral cyber defense initiative, the United States and its allies could strengthen the capabilities of small- to medium-sized enterprises at risk of intellectual property theft and industrial espionage.<sup>31</sup> The Office of the Director of National Intelligence (ODNI), relevant government agencies, and the Federal Bureau of Investigation (FBI) should coordinate with counterintelligence and law enforcement officials in allied countries to gather and analyze data on technology transfers at scale, standardize visa screening procedures, and develop shared standards and metrics to evaluate transactions over the short-, medium-, and long-term.<sup>32</sup> These steps will reduce the vulnerabilities to technology transfer and allow for the sharing of information and best practices. Data collection and analysis will also enable more effective outreach campaigns to raise awareness among allied publics about technology transfer.

Beyond these steps, the United States and its allies should consider establishing AI economic zones that would allow researchers to work in key sectors more freely, provided they abide by a common set of rules. One model is Europe's Schengen Area, which allows for freedom of movement among 26 European states that meet specific criteria. AI economic zones could tether rules about industrial espionage and tech transfer to immigration law: countries that agree to these rules gain freedom of movement or visa waivers, and countries that violate these rules lose certain privileges.

*Optimal Partners:* Germany, the United Kingdom, Japan, Canada, France, and Australia

*Multilateral Fora:* European Union, North Atlantic Treaty Organization (NATO), Multilateral Action on Sensitive Technologies (MAST) conference, ODNI- and FBI-led multilateral dialogues with counterintelligence and law enforcement officials of allied and partner countries

*Criteria for Partnership:* To defend against anticompetitive business practices and stymie the flow of sensitive technical information to China, the United States should work with partners that generate the most technological know-how and seem to attract the most attention in Chinese business and talent acquisition plans.

TABLE 2

## Optimal partners for preventing the transfer of sensitive technical information

	GERMANY	UK	JAPAN	CANADA	FRANCE	AUSTRALIA
Number of Chinese students in country	27,765	96,543	79,375	66,161	24,788	128,498
Number of AI and computer vision publications by researchers based in country	107,102	110,422	127,187	72,144	82,224	46,460
Number of AI and computer vision patents registered in country	308,328	106,790	558,673	57,116	138,218	27,424
Number of information and computer science publications by researchers based in country	219,882	229,682	188,577	140,087	159,611	92,186
Estimated number of AI experts in country	626	1,861	204	1,154	797	657
Number of Chinese professional and tech cooperation associations	46	16	14	23	17	8
Presence of U.S. FBI overseas office	Yes	Yes	Yes	Yes	Yes	Yes
Existing tech transfer policies	Yes	Don't know	Yes	-	Yes	Yes
Concerned about tech transfer	Yes	Don't know	Don't know	-	Yes	Yes
Interest in common tech transfer policies	Yes	Yes	Yes	-	Yes	Yes

Note: "-" indicates no response.

To measure country relevance to combating technology transfer, this study assessed the potential vulnerability of allies and partners by determining how much advanced technical and scientific information each country generates. This assessment included the number of artificial intelligence and computer vision patents and publications tied to researchers based in each country, as well as the number of AI experts (individuals holding PhDs in computer or data science, according to LinkedIn) based in-country.<sup>33</sup>

Next, we assessed potential vectors for technology transfer, including the number of Chinese exchange students and the number of Chinese cooperative technology associations operating in each country.<sup>34</sup> These are crude measurements, since few Chinese students willfully engage in industrial espionage.<sup>35</sup> Yet the Chinese Communist Party does publicly solicit students' help in acquiring trade secrets for Chinese state-owned enterprises in exchange for funding and career advancement opportunities.<sup>36</sup> We measured countries' abilities to thwart industrial espionage—judged in part by the presence of FBI field offices—and willingness to work with the United States.<sup>37</sup> We also included three indicators from the CSET survey: If the country has policies in place to counter tech transfer, expresses concerns about tech transfer, and has an interest in collaborating to counter tech transfer.

*Other considerations and caveats:* Other U.S. allies have relevant expertise in tracking and analyzing technology transfer programs, including the Czech Republic, Italy, the Netherlands, Singapore, South Korea, and Sweden. The United States would benefit from working with as many countries as possible to support data collection and analysis, law enforcement coordination, and public outreach to raise awareness about the risks of technology transfer.

## **Initiative 2: Coordinate investment screening procedures.**

Chinese technology transfer practices manipulate the investment portfolios of state-owned enterprises (SOEs). By making landmark investments in infrastructure, exploiting links in global tech supply chains, and forcing foreign companies to share their intellectual property or localize research and development in exchange for market access, Chinese SOEs have made steady progress in adopting and repackaging cutting-edge science and technology (S&T) products at scale.

All surveyed officials indicated some degree of concern about China's investment in and support of developing countries. Representatives from Japan, France, the EU, Lithuania, the United Kingdom, Australia, the Czech Republic, and Italy expressed a high degree of concern about Chinese investments in developing countries and suggested the United States and its allies should cooperate while creating a level playing field and showcasing a democratic model that is different from Chi-

na. One Italian official noted in the survey that there is a debate in Italy and Europe on this issue and that closer transatlantic partnership could help.

The U.S. Committee on Foreign Investment in the United States (CFIUS) should coordinate with its counterparts in allied and partner countries to build a common intelligence picture of the risks associated with fractional ownership and joint ventures. The starting point for a rigorous approach must be to coordinate investment screening procedures, clarify the transactions posing a national security risk to U.S. and allied supply chains, and establish data-driven criteria for assessing risk.<sup>38</sup>

*Optimal Partners:* the United Kingdom, Germany, Netherlands, France, Italy, and Japan

*Multilateral Fora:* European Union, Joint CFIUS-EU screening meetings, G-7, ODNI- and FBI-led multilateral dialogues with counterintelligence and law enforcement officials of allied and partner countries

*Criteria for Partnership:* When it comes to screening investments, the United States should not limit itself to a selective group of partners: Authoritarian competitors will take the path of least resistance to acquire technology and will increasingly look to alternative suppliers. With limited time and resources, however, the United States should prioritize coordinating investment screening among countries most prone to technology-related investments and acquisitions by Chinese businesses, and most vulnerable to unfair business practices.

To measure the potential vulnerability of allies and partners to Chinese technology transfer through foreign investment, we look to data from the China Global Investment Tracker to approximate Chinese investment in the technology sector of each country over the past three years.<sup>39</sup> We also include a comparison of Chinese tech investment to the net value of foreign direct investment (FDI) inflow over the same period.<sup>40</sup> As a proxy for investment screening capability and willingness, we consider State Department assessments of each country's membership and compliance with multilateral export control regimes, including the Nuclear Suppliers Group, Missile Technology Control Regime, Australia Group, and Wassenaar Arrangement.<sup>41</sup> Finally, we include a measure from the CSET survey: expressed interest in coordinating investment screening procedures with the United States.

*Other considerations and caveats:* Other high-scoring partners include New Zealand, Australia, Finland, and South Korea. Latvia, Lithuania, and Sweden have also established investment screening procedures for critical infrastructure and dual-use technologies.<sup>42</sup> In the survey, a representative from the Czech Republic noted that they may adopt investment screening legislation soon. These steps are important because Chinese initiatives like Belt and Road and Made in China 2025 include a focus on accessing Mediterranean and Eastern European markets. Therefore, the United States and its allies should formulate strategies for bolstering the economic resilience of states in these markets.<sup>43</sup>

TABLE 3

## Optimal partners for coordinating investment screening

	UK	GERMANY	NETHERLANDS	FRANCE	ITALY	JAPAN
Value of Chinese tech-related FDI inflow to country, 2016-2019 (billions of USD)	\$6.28	\$5.17	\$3.83	\$2.57	\$1.01	\$0.81
Value of net FDI inflow (billions of USD)	\$362	\$86	\$192	\$90	\$75	\$38
Participation in multilateral export control groups (NSG, MTCR, Australia Group, and Wassenaar)	4/4	4/4	4/4	4/4	4/4	4/4
Interest in coordinating investment screening with the United States	Yes	Yes	-	Yes	Yes	No

Note: “-” indicates no response.

### Initiative 3: Exploit hardware chokepoints.

Semiconductor devices and integrated circuits are China’s top imports, valued at more than \$260 billion per year (1.5 times more than the country’s oil imports).<sup>44</sup> China cannot meet its domestic demand of semiconductors with indigenous production: 30 percent of its imports are shipped from neighboring Taiwan, and more than 75 percent of the world’s supply of semiconductors are produced by companies based in the United States, Japan, Taiwan, and South Korea.<sup>45</sup> China produces older-generation chips in large quantities, but it is currently unable to manufacture leading-edge chips.

The United States should coordinate with allies and partners to target export controls at supply chain chokepoints that would increase the probability of maintaining China’s dependence on AI chip imports. The United States should work with the Netherlands and Japan on photolithography equipment (the most complex and expensive type of semiconductor manufacturing equipment) and Japan for other types of semiconductor manufacturing equipment, such as deposition, etch, and process control equipment.<sup>46</sup>

In addition, firms headquartered in the United States, Taiwan, and South Korea own all semiconductor fabrication plants producing leading-edge AI chips at scale. If export controls are applied to China on semiconductor manufacturing equipment, the United States, Taiwan, and South Korea should coordinate on the terms under which they will export leading-edge AI chips to China.<sup>47</sup>

*Optimal Partners:* Taiwan, South Korea, Japan, Israel, Singapore, and the Netherlands

*Multilateral Fora:* SEMI, World Semiconductor Council, U.S.-South Korea-Japan Trilateral Strategic Dialogue, G-7, Wassenaar Arrangement

*Criteria for Partnership:* The United States should partner with countries that comprise the backbone of the global supply chain of semiconductors—in particular, advanced integrated circuits with densely packed transistors—and the equipment required to manufacture them.<sup>48</sup>

To measure a country's relevance to the semiconductor supply chain, we included the aggregate value of completed integrated circuits (ICs) each country produces, as well as the ratio of exports destined for China and the United States.<sup>49</sup> In trade relationships where the United States imports a large share of ICs, the producing country may be more willing to implement multilateral controls.

The United States and its partners should leverage chokepoints in the global supply of semiconductor manufacturing equipment (SME): Apart from the United States, only two allies (Japan and the Netherlands) can produce high-end photolithography equipment, and virtually all of the fabrication facilities producing leading-edge, AI-relevant chips are owned by firms headquartered in the United States, Taiwan, and South Korea.<sup>50</sup>

*Other considerations and caveats:* These countries represent nearly the entire world's supply chain of semiconductors and semiconductor manufacturing equipment. Though they do not meet the threshold for being optimal partners, Malaysia and the Philippines also play a role as intermediary destinations for storing and processing many Chinese-bound semiconductors.

## NETWORK TO SEIZE OPPORTUNITIES

### **Initiative 4: Share, pool, and store non-sensitive data sets.**

The United States should work with allied and partner governments to develop common standards for sharing, pooling, and storing non-sensitive, government-owned data sets. U.S. allies and partners are broadly open to non-sensitive data-sharing arrangements: Nearly 90 percent of officials indicated interest in sharing more data with the United States, and 75 percent cited specific non-sensitive data their country would be willing to share. More than half of responding countries indicated a willingness to share weather pattern data, epidemiological data for disease control, medical images for precision medicine, and video and navigation data from self-driving cars. This initiative may be among the most important for America's European partners. An EU official noted that the EU would likely be willing to share quite a lot of data, provided rules are in place and

TABLE 4

## Optimal partners for exploiting hardware chokepoints

	TAIWAN	SOUTH KOREA	JAPAN	ISRAEL	SINGAPORE	NETHERLANDS
Value of integrated circuits exports (USD)	\$170 billion	\$104 billion	\$26.5 billion	\$2.19 billion	\$115 billion	\$5.27 billion
Integrated circuits exports as % of Chinese imports	39%	22%	4.70%	0.70%	9.70%	0.10%
Portion of exported integrated circuits that go to China	47.80%	51.50%	37.00%	66.00%	17.00%	3.10%
Portion of exported integrated circuits that go to U.S.	2.30%	1.70%	4.50%	17.00%	3.70%	0.63%
Percentage of world IC logic production capacity (200mm wafers)	35.60%	7.40%	6.40%	3%	3.90%	0%
Percentage of world IC logic production capacity (quality-adjusted for leading-edge nodes) <sup>51</sup>	69.10%	4.70%	0.10%	7.10%	0.20%	0%
Is in-country photolithography equipment capable of producing at 130nm and below?	No	No	Yes	No	No	Yes
Are in-country fabs capable of producing at 22nm and below?	Yes	Yes	No	Yes	No	No

Note: “-” indicates no response.

enforced. Another official from the UK expressed enthusiasm around the idea of a transnational data sharing framework allowing partners to aggregate more diverse data and create more reliable models that could operate between markets.

Non-sensitive data-sharing projects could start small. The United States, the United Kingdom, and France already cooperate on predictive maintenance for the C-130J military transport aircraft. They could extend this initiative to other aircraft or broaden to include other countries by sharing relevant data collected



during the planning process for maintenance, repair, and overhaul. The United States could partner with Singapore, Spain, Italy, and other NATO allies on a data-sharing initiative related to maritime domain awareness in the way that Indonesia, Malaysia, and Singapore, for example, share hydrographic data and cooperate to improve their anti-submarine warfare capabilities.<sup>52</sup> NATO states that the maritime domain “is of strategic importance.” Its members could share militarily relevant datasets to improve maritime domain awareness in the Black Sea and other strategic locales.<sup>53</sup> U.S. policymakers could also work with counterparts in allied and partner countries to develop common standards for data archival procedures, including standards for ensuring the data is labeled, stored, interoperable, and accessible.<sup>54</sup> The U.S. Open Government Initiative began to lay the groundwork for common data standards as early as 2013, and the United States should promote similar practices among allies and partners.<sup>55</sup> Such a collaborative approach would enable data flows and promote healthy data management among allies that could further propel the growth of AI.

*Optimal Partners:* United Kingdom, Germany, Japan, France, the Netherlands, and New Zealand

*Multilateral Fora:* NATO, the European Commission, Five Eyes, OECD, Association of Southeast Asian Nations (ASEAN)

*Criteria for Partnership:* Optimal data-sharing partners would be countries that widely collect and publish data for public use, and countries where that data is stored and accessible by third parties.

To assess capability and compatibility, we selected metrics reflecting the amount of data that allied and partner governments generate and capture. We included data from the Open Knowledge Foundation’s Global Open Data Index, which measures the volume and types of publicly available government data, such as national statistics, procurement practices, air quality and weather information, and company registry information.<sup>56</sup> We also included the number of data processing centers in each country and the gross value of imported data storage units.<sup>57</sup> While it is difficult to determine what kind of data they store or how much storage capacity they have, the dollar value of data processing and storage centers is a reasonable proxy for national data capacity and reflects the amount of data generated by entities in each country. Moreover, we featured three indicators from the CSET survey: expressed interest in data sharing with the United States, whether the country has taken actions to enhance data archival procedures, and whether it has established data use standards.

Finally, we compared legal environments in each country as they pertain to data sharing.<sup>58</sup> Although all the countries listed in Table 5 fall under the jurisdiction of the EU’s General Data Protection Regulation (GDPR), they have no apparent localization requirements, nor do they prevent the transfer of certain classes of data across borders.<sup>59</sup> Moreover, shared data standards under the GDPR may make it easier for the United States to collect the same kind of data from multiple countries in the future.

*Other considerations and caveats:* Other high-scoring countries include South Korea, Finland, Denmark, Lithuania, Latvia, and the Czech Republic. The United States would do well to diversify its sources of data, including from countries beyond the jurisdiction of the GDPR. India, for example, boasts a large population, vibrant technology market, and high concentration of data processing facilities.

TABLE 5

## Optimal partners for sharing, pooling, and storing non-sensitive data sets

	UK	GERMANY	JAPAN	FRANCE	NETHERLANDS	NEW ZEALAND
Global Open Data Index (top score 0.9)	0.79	0.51	0.61	0.7	0.54	0.68
Number of colocation data centers	415	417	200	249	251	73
Value of data storage unit imports (USD)	\$6.05 billion	\$11.3 billion	\$6.82 billion	\$4.79 billion	\$5.64 billion	\$0.55 billion
Stringency of data protection laws	Heavy	Heavy	Robust	Heavy	Heavy	Robust
Consent required for transfer of personally identifiable data?	Yes	Yes	Yes	Yes	Yes	Yes
Any type of data localization apparent?	No	No	No	No	No	No
General Data Protection (GDPR)-adequate country?	Yes	Yes	Yes	Yes	Yes	Yes
Interest in data sharing with U.S.	Yes	Yes	Yes	Yes	-	-
Action to improve data archival procedures	Don’t know	Don’t know	Yes	Yes	-	-
Action to create data use standards	Yes	Don’t know	Yes	Yes	-	-

Note: “-” indicates no response.

### **Initiative 5: Invest in privacy-preserving machine learning.**

To protect individual privacy, the United States and its allies and partners should explore techniques in data analysis that would allow them to perform operations on non-sensitive data sets without sharing or storing personally identifiable information. These techniques are known as privacy-preserving machine learning. Researchers Roxanne Heston and Helen Toner observe that privacy-preserving machine learning could make “new uses of AI possible without triggering privacy concerns, give U.S. companies a competitive edge over their foreign counterparts, and/or reduce cybersecurity risks by protecting individual data while preserving its usefulness.”<sup>60</sup> Applications of privacy-preserving machine learning could include performing object and facial recognition locally on an individual’s phone instead of processing that data in the cloud, thereby improving security and privacy; employing differential privacy models to obscure the identities of individuals in census research; and using secure multi-party computation to combat tax fraud.<sup>61</sup>

Coordinated investment initiatives in homomorphic encryption, secure multi-party computation, and federated learning would enable democratic, market-based economies to benefit from larger and more diverse pools of data without compromising the privacy of individual users and organizations whose data are in the pools. U.S. allies and partners are especially willing to collaborate on this front. Nearly all surveyed officials indicated interest in collaborating on an international certification scheme for the protection of personal data, with two-thirds of surveyed officials indicating high interest. As Australia’s AI Ethics Framework notes, “Throughout their lifecycle, AI systems should respect and uphold privacy rights and data protection, and ensure the security of data.”<sup>62</sup>

The United States and its allies should discuss potential use cases where privacy-preserving machine learning could be developed and deployed, coordinate research and development priorities that further applications suitable to these technologies, and create guidelines and technical standards to promote safe and reliable applications in realistic scenarios.<sup>63</sup>

More broadly, the United States and its allies should co-fund research and coordinate investments into new techniques, such as synthetic data, advanced simulations, and improvements in transfer learning, for making personal data less relevant to AI systems.

*Optimal Partners:* Canada, India, Germany, Australia, Japan, and the United Kingdom

*Multilateral Fora:* EU, OECD, the Quadrilateral Security Dialogue (India, Japan, Australia, and the United States), National Institute of Standards and Technology- and National Science Foundation (NSF)-led bilateral and multilateral partnerships

*Criteria for Partnership:* The United States should coordinate with countries whose scientists produce most of the world's cutting-edge AI research focused on privacy and anonymity, such as homomorphic encryption and federated learning techniques. Ideal partners would also respect online privacy and share U.S. concerns about digital illiberalism.

To measure countries' relative strengths in privacy-preserving machine learning, we counted the number of patents and scientific publications from scientists affiliated with local research institutions. We only assessed patents and publications labeled as relevant to artificial intelligence and computer vision applications that explicitly mention "privacy" or "anonymity."<sup>64</sup> We included Freedom House's scores of internet freedom in each country as a proxy for governments' commitments to democratic values and civil liberties.<sup>65</sup> We also aggregated four measures from the CSET survey to capture countries' focus on privacy: expressed interest in an international scheme for the protection of personal data, government action taken to enhance privacy protections, perceptions of the need for international management of facial recognition, and the country's likelihood of regulating surveillance technology.

*Other considerations and caveats:* France and South Korea produce a large number of AI patents related to privacy and score highly on Freedom on the Net. U.S. policymakers could also consider partnering with individual tech companies abroad to further privacy-preserving research projects. The frequency of the phrase "privacy" in national AI strategies is a crude measure: India and the United Kingdom score "0," for example, but both countries are likely deeply concerned about privacy issues.

#### **Initiative 6: Promote interoperability and agile software development.**

Interoperability is a critical lubricant for U.S. alliances. To operate effectively, allies need to plan, train, and exercise together. Joint operational concepts, common doctrine, and compatible military capabilities and systems are required to communicate effectively and achieve shared objectives.<sup>66</sup> As countries integrate AI into military systems, the United States and its allies must ensure that hardware and digital systems are interoperable and secure.

The United States and its allies could start with common standards for interoperability, safety, and security of AI systems, including AI-enabled, safety-critical systems.<sup>67</sup> For AI-enabled military systems expected to perform a given function, the United States and its allies should agree on common benchmarks for accuracy and performance based on the same training and testing data. The CSET survey suggests that allies and partners desire such benchmarks, with a majority of surveyed officials expressing the need for international coordination and management of AI military applications, specifically autonomous weapons systems and unmanned

TABLE 6

## Optimal partners for coordinating investment in privacy-preserving machine learning

	CANADA	INDIA	GERMANY	AUSTRALIA	JAPAN	UK
Number of AI and image processing publications mentioning "privacy" or "anonymity"	3,730	7,439	4,710	3,206	3,053	6,064
Number of AI and image processing patents mentioning "privacy" or "anonymity"	1,294	527	1,280	833	1,888	994
Frequency of phrase privacy/100 words in national AI strategy	0.7	0	0.04	0.24	0.29	0
Freedom House score of Freedom on the Net (0 = most free)	15	43	19	21	25	23
OECD score of trust in the Internet	2.66	2.58	2.73	2.9	2.25	2.29
Percent of people "somewhat" or "very" concerned about online privacy	76%	92%	67%	74%	72%	72%
Interest in international personal data protections	-	-	Yes	Yes	Yes	Yes
Action to enhance privacy protections	-	-	Yes	Yes	Yes	Yes
Need for international management of facial recognition	-	-	Yes	Yes	No	Yes
Likelihood of regulating surveillance tech	-	-	Extremely likely	Don't know	Extremely unlikely	Don't know

Note: "-" indicates no response.

vehicles for submarine detection. A German representative stated that collaboration with the United States would be enhanced by an AI strategy that includes a focus on AI-related defense and security threats.

The United States and its allies should also consider wargaming and table-top exercises to explore how sharing selected government data sets could shore up defenses against counter-AI techniques and other efforts to exploit the vulnerabilities of AI systems. Specifically, they should explore how sharing militarily relevant data sets and certain AI algorithms could help allied countries better test system robustness, expose mutual vulnerabilities, accelerate development of countermeasures, and establish common standards for testing, verification, and validation.<sup>68</sup>

The United States and its allies should define common standards for the level of robustness required for a given operation. Common defense planning and capability development in NATO and the EU should give priority to investments in AI safety and security, as well as common verification procedures for AI-enabled, safety-critical systems.

To ensure allies store and process data homogeneously, the United States and its allies should launch an accelerator fund for cloud computing. The United States and its allies could use this fund to more efficiently procure commercial cloud computing technology. The United States, United Kingdom, and Canada, for example, could agree to bid out a bulk purchase of cloud compute from major technology companies and distribute access to compute in the form of credits and publicly funded research. This initiative would ensure that democratic nations benefit from techniques in machine learning that require fewer inputs of real-world data but greater computational power to run simulations and self-play methods. Representatives from Japan, South Korea, the Czech Republic, Lithuania, and the EU each cited increased computing as an AI R&D priority, suggesting an area for aligning focus among allies.

Parallel to this effort, the United States and its allies should launch a software development initiative. This initiative could take a page out of the U.S. Air Force's Kessel Run project by pairing government-led teams with software developers from allied countries. Multinational teams could work together to build capabilities in agile software used in military systems that are part of joint exercises. Allies could also use AI to automatically create "translators" between systems and user interfaces that are not yet fully interoperable. The United States and its NATO allies should consider partnering with existing frameworks like the AI4EU artificial intelligence test bed, which pools compute and data among EU countries.<sup>69</sup>

*Optimal Partners:* Canada, Australia, United Kingdom, Germany, Italy, and Japan

*Multilateral Fora:* Five Eyes, NATO, NATO-EU (AI4EU) test bed partnership, U.S.-Japan-South Korea Trilateral Defense Cooperation, National Technology and Industrial Base (Australia, Canada, the United Kingdom, and the United States)

*Criteria for Partnership:* The United States should improve technical interopera-

bility with the countries that receive the most attention in U.S. global security operations, interact the most with U.S. forces, and express the most concern about disjointed technical requirements and capabilities.

We expected countries interfacing most with U.S. forces to host U.S.-owned military bases, contribute personnel and equipment to NATO exercises, purchase large amounts of U.S. military hardware, or enjoy collective defense arrangements with the United States.<sup>70</sup> We recorded which countries take part in four multilateral security arrangements, including whether each country is a member of NATO or designated a major non-NATO ally, party to the Proliferation Security Initiative (PSI), the Global Coalition to Counter Daesh, or the Global Counterterrorism Forum.<sup>71</sup> We also chose to highlight members of the National Technology and Industrial Base, a legal designation reserved for allies who “support national security objectives of the United States, including supplying military operations,” “conduct advanced R&D,” and “develop industrial preparedness to support operations in wartime or a national emergency.”<sup>72</sup>

Finally, we used a proxy indicator to assess the importance of interoperability for each country by measuring how frequently their national AI strategy documents mention phrases related to “interoperability,” “cooperation,” “collaboration,” and “security,” or positively mention working with the United States.

*Other considerations and caveats:* The United States should not limit its attention to the aforementioned countries; the Joint Chiefs of Staff seek to develop a “capability-focused, effects-based interoperability process” among all relevant security partners and allies.<sup>73</sup> Other high-scoring countries in our sample included Denmark, Spain, South Korea, and other NATO allies. Additionally, the keyword searches we conducted of national AI strategy documents are not definitive measures of a country’s strategic commitment to the United States.

### **Initiative 7: Launch an AI R&D collaboration challenge.**

The United States and its allies account for nearly two-thirds of global R&D spending, including public and private R&D investment.<sup>74</sup> Policymakers need to think about how to leverage this pool of R&D and deploy it in areas that will enable them to develop economically, innovate collaboratively, and strengthen liberal democratic values. The United States may at times compete with its allies in attracting top AI talent and promoting favorable ecosystems for research and development. While these tensions are real, they are also surmountable.

When the NSF or DARPA fund AI research, they put out calls for research into specific subfields or functions of AI. The U.S. government can expand coordination with foreign science funding organizations (e.g. NSF counterparts abroad, such as the European Research Council) to solicit research on complementary agendas,

TABLE 7

## Optimal partners for promoting interoperability and agile software development

	CANADA	AUSTRALIA	UK	GERMANY	ITALY	JAPAN
Defense agreement with United States?	Yes	Yes	Yes	Yes	Yes	Yes
Value of arms imports from United States (2016-2018, USD)	\$436 million	\$2,895 million	\$1,116 million	\$10 million	\$1,013 million	\$1,415 million
Member of the National Technology and Industrial Base (NTIB)?	Yes	Yes	Yes	No	No	No
Number of U.S.-operated military bases in-country	0	1	5	9	6	13
Member of NATO or designated major non-NATO ally?	Yes	Yes	Yes	Yes	Yes	Yes
Country contributes > 1% of non-U.S. personnel or equipment in current NATO operations?	Yes	Yes	Yes	Yes	Yes	No
Participation in multilateral security arrangements	4/4	4/4	4/4	4/4	4/4	4/4
Frequency of "interoperable" per 100 words in national AI strategy	0	0	0.013	0	0	0.004
Frequency of "cooperation" per 100 words in national AI strategy	0	0.3	0.01	0.33	0.35	0.04
Frequency of "collaboration" per 100 words in national AI strategy	2.24	0.11	0.22	0.01	0	0.2
Frequency of "security" per 100 words in national AI strategy	0.56	0.24	0.09	0.02	0	0.08
Net positive- valence mentions of "United States" in national AI strategy	0	3	20	0	0	9

such as human-machine teaming methods and verification techniques for complex control systems and AI-enabled, safety-critical infrastructure.<sup>75</sup>

Collaboration is especially useful when allies make breakthroughs or relative progress in specific areas, such as autonomous vehicles and industrial applica-



tions in manufacturing and service provision. Annual meetings of performers could provide a forum for collaboration on future calls or the identification of common agendas among distinct research communities. For example, the AI4EU test bed is an EU-specific initiative to pool government resources from many countries and fund individual AI researchers. The United States and its allies should explore such innovative models with countries in Europe and elsewhere.

Most AI research and development takes place in the private sector or academia. As a result, the U.S. government will need to become a “fast follower” and ready-adopter of commercial innovations. By creating a consortium of industry, academia, and government across allied nations, the United States and its partners could better leverage expertise and funding.<sup>76</sup>

Close partnership among government, industry, and academia is essential not only for maintaining but strengthening American competitiveness in AI. U.S. policy-makers should consult regularly with important domestic and foreign companies and even individual AI researchers. The CSET survey finds that partners rely heavily on domestic industry and academia to develop national AI R&D priorities. All surveyed officials indicated a significant role for industry in shaping government priorities and R&D decisions, specifying that industry consultations occur on a regular basis. Officials’ open-ended responses highlighted institutionalized and informal channels of public-private coordination, which they considered critical in driving AI R&D forward.

U.S. policy can support a robust private sector by increasing federal R&D, especially in AI safety, security, and other areas the private sector is less likely to emphasize; creating incentives for private-sector AI R&D; providing critical enabling infrastructure, such as access to compute and shared public data sets; supporting the development of AI talent; and promoting favorable ecosystems through public-private partnerships and innovation clusters. Untapped opportunities exist for the United States to work with its international partners to share best practices, expand research networks, and open up new markets for companies and researchers to advance the competitiveness of democratic nations in AI.

*Optimal Partners:* Japan, Germany, South Korea, France, United Kingdom, and the Netherlands

*Multilateral Fora:* EU, MAST conference; OECD; ASEAN; NSF-, National Institutes of Health (NIH)-, and Department of Energy (DOE)-led innovation dialogues

*Criteria for Partnership:* To capitalize on allied technology research and development, the United States should give priority to working with countries that generate the lion’s share of AI research and investment. U.S. academic and industrial research hubs can take advantage of long-standing, global networks of research partnerships to remain competitive.

There are myriad ways to measure national research and development capability. We focus on investment, scientific publications, patents, and IP environments. On investment, we captured national aggregate R&D funding across all sectors, as well as private sector investments in information and communication technologies (ICT).<sup>77</sup> For scientific publishing activity, we referenced the Nature Index, a database of author affiliation information from 82 leading science journals.<sup>78</sup> The Nature Index quantifies contributions made to scientific journals by co-authors from various countries.<sup>79</sup> Although not directly related to AI or computer science publications, the Nature Index data is a reliable indicator of cross-border university partnerships and scientific collaboration, including the strength of each country's academic relationships with the United States and China (partner rank).

Beyond the Nature Index, we recorded whether each country hosts an institution affiliated with the National Science Foundation or the Partnership on AI.<sup>80</sup> We also included composite scores from the U.S. Chamber of Commerce<sup>81</sup> and the International Property Rights Index to measure the strength of and compliance with intellectual property protections in each country.<sup>82</sup> Both indices compile dozens of indicators of the strength of intellectual property protections in each country, measuring qualities like business perceptions of IP protection and incidences of copyright piracy. We also counted the number of computer technology patents filed in each country as a measure of research productivity.<sup>83</sup> Finally, we included one measure from the CSET survey: the significance of industry in national AI R&D priority setting.

*Other considerations and caveats:* From industry reports, other global R&D hubs include Ireland, Australia, and Canada. The United States may want to accord special weight to countries with world-class AI research outfits, such as Canada's Vector Institute. It is difficult to measure how much business enterprise or public sector R&D in each country is dedicated to AI. In addition, scientific partnerships between countries in the physical sciences may not map to artificial intelligence and computer science.

### **Initiative 8: Develop inter-allied human capital for AI.**

The global competition for AI talent is nominally zero-sum, but talent development efforts such as education and training could expand it. The United States should cultivate international networks of researchers through exchange programs. One potential model is the U.S. Telecommunication Training Institute, which brings officials from developing countries to the United States for tuition-free training in information and communications technologies. Such programs would enable U.S. and allied policymakers to identify comparative advantages in AI, share best practices, and promote linkages and the free flow of ideas between government, industry, and academia.

TABLE 8

## Optimal partners for launching an AI R&amp;D collaboration challenge

	JAPAN	GERMANY	SOUTH KOREA	FRANCE	UK	NETHERLANDS
Value of business enterprise R&D in ICT (USD)	\$26.35 billion	\$14.39 billion	\$28.02 billion	\$7.50 billion	\$4.80 billion	\$2.01 billion
Aggregate data on national R&D spending (USD)	\$185.53 billion	\$114.84 billion	\$85.43 billion	\$62.13 billion	\$49.16 billion	\$18.64 billion
Scientific publishing activity score (Nature Index)	1,659.61	5,089.52	813.49	2,606.94	4,399.28	1,206.93
U.S. scientific collaboration partner rank	1st	1st	1st	1st	1st	1st
China scientific collaboration partner rank	2nd	5th	2nd	5th	4th	4th
National org partners with NSF?	Yes	Yes	Yes	Yes	No	No
Member of Partnership on AI?	Yes	Yes	No	Yes	Yes	Yes
Score on U.S. Chamber International IP index (max score 45)	34.6	36.5	33.2	36.7	37	35.3
Score on International Property Rights Index (max score: 8.7)	8.3	7.9	6.6	7.4	8	8.3
Number of computer tech patent publications by applicant origin (2018)	24,668	5,432	16,222	3,249	2,538	1,922
Industry significance in national AI R&D priorities	Very significant	Moderately significant	Very significant	Moderately significant	Very significant	-

Note: “-” indicates no response.

The right approach would facilitate the exchange of knowledge and best practices among allied and partner countries. The NSF, for example, has awarded grants to researchers who seek to promote international collaboration and benefit from the expertise and specialized skill sets of international partners.<sup>84</sup> Additional

programs, joint scholarships, and conference support could synchronize efforts to grow the pool of AI talent. Survey results suggest that partners already engage in various efforts to leverage international ties to encourage STEM education, provide AI-relevant fellowships, and offer AI-specific advanced and technical degrees.

Exchanges and fellowship programs could also mitigate zero-sum dynamics, such that when a country “loses” AI talent to an ally or partner, it nevertheless gains from the capabilities and networks of which its researchers are a part. To further this effort, the U.S. government should commit resources to hosting and convening workshops among AI researchers, fostering international networks of AI researchers, and deepening partnerships with existing networks, such as the Confederation of Laboratories for Artificial Intelligence Research in Europe (CLAIRE). The United States and its allies should coordinate with the private sector from the outset on job placement and training programs, including hosting recruiting sessions that bring together representatives from government, industry, and academia. Surveyed officials from the United Kingdom, Chile, Colombia, and Japan noted ongoing public-private partnerships to foster AI talent, including providing subsidized training courses, promoting women in STEM, and talent development programs.

*Optimal Partners:* India, the United Kingdom, Germany, France, Canada, and South Korea

*Multilateral Fora:* Institute of Electrical and Electronics Engineers, U.S. Telecommunication Training Institute- or CRDF Global-like exchange programs, and NSF international partnerships

*Criteria for Partnership:* U.S. AI enterprises should focus on training the world’s best and brightest AI researchers, while also attracting up-and-coming overseas talent. Ideal sources of talent include countries that place premiums on scientific and mathematical education, and those where the world’s leading AI researchers are based.

We measured AI human capital in several ways to capture students and experts. Element AI measures AI experts by country, counting the number of people with PhDs on LinkedIn and whether they presented at major AI conferences.<sup>85</sup> We also used UNESCO data to estimate the total number of outbound, internationally mobile college graduates with STEM and ICT degrees from each country.<sup>86</sup> In countries producing the highest number of STEM undergraduate degree holders—like Germany—students are choosing to stay in-country after graduation. Talent immobility implies that temporary cross-border training opportunities like summer workshops may be the best way to create talent networks among allies. We also included an indicator from our survey to measure country investment in AI talent: whether the country has programs in place to train domestic talent, attract international AI talent, or both.

*Other considerations and caveats:* Australia and Spain are also home to many

TABLE 9

## Optimal partners for developing inter-allied human capital for AI

	INDIA	UK	GERMANY	FRANCE	CANADA	SOUTH KOREA
Number of data science and ML researchers working in-country (LinkedIn)	798	3,387	1,351	1,426	1,487	192*
Number of AI researchers working in-country who presented at conferences (2018)	555	1,475	935	695	815	405
Number of yearly higher ed and vocational graduates in ICT	431,573	27,306	27,951	23,415	12,238	28,655
Number of yearly higher ed and vocational graduates in STEM	2,751,276	198,532	200,671	197,522	89,578	189,620
Number of yearly outbound, internationally mobile STEM or ICT higher ed and vocational grads	125,376	10,555	50,173	25,553	11,956	36,289
Program(s) to train/attract AI talent	-	Yes	Yes	Yes	Yes	Yes

Note: "\*" indicates that a number may be inaccurate due to low LinkedIn penetration or English language use.

Note: "-" indicates no response.

of the world's leading AI researchers and produce many of the world's AI-related patents. Some metrics in this section may not adequately represent the global distribution of AI talent. For example, although India appears to produce a huge number of tertiary education graduates, many graduate from two-year vocational programs and technical apprenticeships, which may not be as relevant to AI development. LinkedIn penetration is also low outside the Anglophone world, potentially skewing maps of AI experts to favor English-speaking countries.

## PROJECT INFLUENCE

### Initiative 9: Shape global norms and standards for AI.

The United States has a vested interest in setting the rules of the road for artificial intelligence. Western countries have already taken the lead in developing principles governing the application of artificial intelligence. China has produced its

own set of principles and engages actively in international bodies, such as the International Telecommunication Union (ITU) and the 3rd Generation Partnership Project (3GPP), to establish standards for mobile network technologies and the future governance of AI.

By assuming leadership in AI, the United States and its allies face risks and opportunities. The risks are twofold. On the one hand, standard setting could become a casualty of geopolitical competition as leading countries precipitate a race to the bottom. On the other hand, China already asserts its principles and standards through a variety of multilateral fora. The opportunity is that the United States and its allies can act now to set global standards for AI reflecting and supporting human rights and liberal democratic values, while addressing critical questions surrounding the rollout of 5G, facial recognition for surveillance, automated cyber exploitation and defense, and autonomous weapons systems. A Japanese official responding to the CSET survey noted that the United States and its allies should adopt a citizen-centric AI strategy. Such citizen-centric strategies would seek to develop and deploy AI for the benefit of democratic societies, including strengthened data privacy standards and respect for civil liberties; economic empowerment of citizens within rules-based market economies; greater access to education, precision medicine, energy efficiency, and more inclusive social service provision.

The United States should lead a multilateral effort with allies and partners to set international rules of conduct for AI. This effort should build on and extend the OECD Principles on AI and the International Organization for Standardization working group initiatives on standards for data and AI safety and security. The United States and its allies could establish a standing platform to coordinate policies on standard-setting in multilateral fora. This is likely an area for productive dialogue, as partners are eager to coordinate policies and share best practices around norms and standards. In fact, all surveyed officials were extremely or very interested in this avenue for international collaboration.

Longer term, the United States and its allies should explore the conditions for a common AI market, including standards for testing, verification, and validation of AI technologies, as well as common practices for certifying companies that support liberal democratic values and privacy.<sup>87</sup> This common market would create incentives for other countries to abide by these principles in the development and deployment of safe and reliable AI. As one EU representative observed, if the West could offer a viable way of doing AI that respects privacy and fundamental rights, developing (and democratic) countries would be more inclined to follow the Western model.

*Optimal Partners:* Canada, United Kingdom, Ireland, Australia, Singapore, and Japan

*Multilateral Fora:* EU, OECD, International Organization for Standardization and International Electrotechnical Commission Joint Technical Committee 1 Sub Committee 42 – Artificial Intelligence, WTO, 3GPP, NATO-EU joint initiative on standards for emerging technologies

*Criteria for Partnership:* To lead the global discussion on AI safety and ethics, the United States will need to build a coalition of like-minded, influential countries from which it can listen and learn and with whom it can shape norms and standards. Ideal partners will be countries that host active and engaged civil societies, who have historically aligned with liberal democratic values and U.S. policy priorities, and who most actively collaborate internationally to develop AI norms and standards.

Allies that more frequently use information and communication technologies, issue governance documents about AI, and host robust public sector discussions about AI and image recognition are optimal partners for shaping global norms, standards, and best practices around these technologies. For one measure of technology use, we included the World Economic Forum’s Government Usage of ICT index, as well as a count of national AI governance documents provided by Nesta.<sup>88</sup> We also measured commitment to a democratic way of AI by canvassing national AI strategies for mentions of “principles,” “norms,” “standards,” and “safety.” To measure international clout and diplomatic capacity, we captured the number of diplomatic posts each country operates worldwide, as well as their ranks on the Soft Power 30 Index.<sup>89</sup> Finally, we recorded countries’ demonstrated willingness to ban technology imports from Huawei Technologies as a proxy for their willingness to work with the United States.<sup>90</sup>

*Other considerations and caveats:* The United States will need to expand cooperation beyond the aforementioned countries to promote liberal democratic norms and standards for AI. Sweden and New Zealand were among the top-scoring countries for this initiative. As the world’s largest democracy, India is also an important partner in this effort. Policymakers will need to weigh additional considerations: countries that generate a high quantity of policy documents about AI may not make for optimal partners if these documents do not align with U.S. values and policy priorities. What’s more, many national guidelines mention or touch on AI but are not directly related to AI, and data is not widely available for non-Anglophone countries.

TABLE 10

## Optimal partners for shaping global norms and standards for AI

	CANADA	UK	IRELAND	AUSTRALIA	SINGAPORE	JAPAN
Number of governance documents about AI	7	23	1	1	5	5
Score on government usage of ICT index (max score 6.3)	5.1	5.4	4.9	5	6.3	5.4
Number of diplomatic posts worldwide (diplomatic capacity)	147	225	80	116	49	229
Rank on Soft Power 30 Index	7th	2nd	-	9th	21th	8th
Frequency of word principles/100 words in national AI strategy	0.56	0	0.31	0.24	0	0
Frequency of word norms/100 words in national AI strategy	0	0	0	0.02	0	0
Frequency of word standards/100 words in national AI strategy	0.56	0.04	0.78	0.16	0.34	0.1
Frequency of word safety/100 words in national AI strategy	0.28	0.08	1.72	0.17	0.11	0.06
Frequency of word democracy/100 words in national AI strategy	0.56	0.02	0	0	0.11	0
Frequency of phrase human rights/100 words in national AI strategy	0.42	0	0	0.07	0.11	0
Has country banned Huawei products?	No	No	No	Yes	No	Yes
Does Huawei contract with 5G provider?	No	Yes	Yes	No	No	No

Note: “-” indicates no response.



### **Initiative 10: Establish a multilateral digital infrastructure network.**

One of the chief attractions of Chinese-supplied consumer technologies (5G, cell phones, computers, digital wallets) is that they are less expensive than Western equivalents, and market access is often a condition for Chinese companies investing in developing countries. For example, some allies and partners are reluctant to ban Huawei for fear of losing access to the Chinese market and investments. Even among partners, the appeal of cost effectiveness sometimes outweighs considerations of privacy and security. The CSET survey found that cost effectiveness matters more than privacy for international agreements around software contracts. Yet privacy matters more among partners for international agreements around data storage and sharing. Surveyed officials were split in terms of the relative importance of privacy and cost for international agreements around novel applications and hardware investment. Germany, Australia, and the EU tended to favor privacy in all cases, while Colombia and the Czech Republic tended to favor cost effectiveness when considering international collaboration.

To promote a rules-based global trading order, the United States should not mimic China's model of state-driven, top-down national development strategies that trade investment for market access. Instead, the United States should form a multilateral consortium to coordinate the extension of credit to European mobile telecommunications networks and invest in next-generation networks.<sup>91</sup>

The United States and its allies should also launch a multilateral digital infrastructure network. This network could be modeled on USAID's Higher Education Solutions Network, a partnership between USAID and development labs at seven major universities, and the EU's Digital4Development policy, an initiative that harnesses information and communications technologies to promote sustainable development.<sup>92</sup> A multilateral digital infrastructure network would enable the United States and its allies to partner with developing countries to build digital capacity in support of the UN's Sustainable Development Goals. The right approach would ensure that digital systems in emerging markets are open, secure, resilient, and interoperable, while empowering developing countries to protect data privacy, meet their domestic needs, and access high-performance computing and mobile internet technologies.

Liberal democratic governments have established frameworks and standards for good governance tied to development lending and giving. Democratic countries should include AI in these frameworks along with capacity building to ensure that developing countries can make sovereign and democratically accountable decisions about the deployment of AI. Many developing countries are growth markets and present opportunities to shape AI governance consistent with liberal democratic principles. As part of this effort, the United States and its allies should integrate federated learning techniques and data privacy into digital capacity building efforts with developing countries. By creating an accelerator fund for privacy-preserving

machine learning technologies, the United States and its allies could promote an alternative model of development that puts data protection and privacy at the absolute center.

*Optimal Partners:* Germany, Japan, France, United Kingdom, Ireland, and Canada

*Multilateral Fora:* IMF, World Bank, European Bank for Reconstruction and Development, Asian Development Bank, and Digital Nations (The Digital 9)

*Criteria for Partnership:* The best partners for investing in global digital infrastructure are countries that lead in foreign aid and consider technology to be a staple of development and governance.

We measured outflows of official development assistance (ODA) and foreign direct investment (FDI) from each country. We considered three indices of governments' commitment to technology and global development: the UN e-Government Development Index, the Digital Evolution Index, and "technology" scores on the Commitment to Development Index.<sup>93</sup> We also included a measure from our survey: expressed concern around China's investments in the developing world.

TABLE 11

## Optimal partners for establishing a multilateral digital infrastructure network

	GERMANY	JAPAN	FRANCE	UK	IRELAND	CANADA
Score on Commitment to Development Index - Technology (higher is better)	5.32	5.53	5.43	4.66	4.11	5.04
Number of points on e-Government Development Index (higher is better)	0.88	0.88	0.88	0.9	0.83	0.83
Value of FDI outflows (BoP, billions of USD)	\$159.1 billion	\$159.1 billion	\$126.2 billion	\$43.2 billion	\$94.4 billion	\$52.6 billion
Value of ODA (net, billions of USD)	\$25 billion	\$11.5 billion	\$11.3 billion	\$18.1 billion	\$0.8 billion	\$4.3 billion
Value of Score on Digital Evolution Index as of 2017 (higher is better)	3.36	3.52	3.25	3.67	3.41	3.55
Concern about Chinese investment in developing countries	Yes	Yes	Yes	Yes	-	-

Note: "-" indicates no response.

*Other considerations and caveats:* Other high-scoring countries included South Korea and Sweden for their commitments to digital development. It is also important to consider the optimal destinations for digital infrastructure support. Ideal recipients would be countries at risk of becoming dependent on Chinese technology and monetary assistance, for whom price is a prohibitory factor in buying from companies based in the United States and allied countries. As of this writing, China's Belt and Road Initiative encompasses more than 60 countries.<sup>94</sup>



# Conclusion

**H**ow can the United States collaborate with allies and partners to shape the trajectory of AI in ways that will promote liberal democratic values and protect against authoritarian uses of this technology?

The evidence in this report suggests alliances are relevant to defending against Chinese and Russian efforts to wield AI for authoritarian ends, networking with partners to advance technological progress, and projecting shared democratic values in the age of AI.

Forging a democratic way of AI requires blending two strategic approaches: signaling and shaping.<sup>95</sup> The United States needs to formulate policies that signal resolve to strategic competitors and reassurance to allies and partners. By pursuing the initiatives outlined in this report, the United States can communicate resolve through sensible policies, smart investments, and clarity about intentions. Equally important, the United States will need to deepen cooperation with allies and partners to shape the ecosystems for development and deployment of safe and reliable AI.

By coordinating with allies and partners to counter technology transfer, leverage hardware chokepoints, invest in privacy-preserving machine learning, share non-sensitive data sets, foster R&D collaboration, develop human capital, enhance interoperability, promote global norms and standards, and establish a digital infrastructure network, the United States and its allies can shape the global environment in ways that support democratic values. The stakes are clear, and the stage is set for the United States and its allies to rise to the challenge.



## Appendix I. Survey Methodology

The survey was fielded online from October–November 2019. It was sent to 60 official representatives from 27 countries plus the European Union. Fifteen representatives completed the survey, a response rate of 25 percent, representing 11 contacted countries and the European Union (42 percent).

The survey employed a non-random, snowball sampling procedure. Countries were chosen based on their current participation in a mutual defense treaty, strategic partnership, or cooperative defense agreement with the United States, and their development of, or expressed plans to develop, a national AI strategy. We employed this selection criteria because we were interested in the AI priorities and perspectives of potential allies and partners with some degree of capability and compatibility with U.S. values and interests. The priorities and preferences of countries not engaged in multilateral or national conversations around AI are beyond the scope of this research. We also intentionally included a range of geographical regions (e.g. Europe, Asia, Latin America).

Country officials were chosen by their position within their respective governments. We focused on personnel from science and technology agencies and foreign ministries or embassies. We employed this selection criteria because these are the officials best equipped to speak to the country's AI goals. Specific representatives were identified through agency websites, online directories, and references.

Identified representatives were invited to participate via email and completed the survey online through the Qualtrics Survey Platform. The survey included 27 questions about AI R&D priorities, international coordination and data sharing preferences, talent development strategies, and perceptions of other country's approaches to AI. A personalized reminder was sent by email to representatives who had not completed the survey two weeks after the initial invitation and a final reminder was sent two weeks later. Table A lists the countries invited to participate in the survey, the number of representatives contacted, and the number of responses received for each country.

TABLE A

## Survey Responses by Country

COUNTRY	# OF REPRESENTATIVES CONTACTED	# OF RESPONSES
Australia	6	2
Austria	2	0
Canada	4	0
Chile	1	1
Colombia	3	2
Czech Republic	1	1
Denmark	2	0
Estonia	1	0
European Union	1	1
Finland	2	0
France	6	2
Germany	2	1
India	4	0
Ireland	1	0
Israel	1	0
Italy	1	1
Japan	3	1
Latvia	1	0
Lithuania	1	1
Malaysia	1	0
Mexico	1	0
Netherlands	2	0
New Zealand	1	0
Singapore	2	0
South Korea	2	1
Spain	1	0
Sweden	2	0
United Kingdom	5	1
<b>Total: 28</b>	<b>60</b>	<b>15</b>



## Appendix II. Methodology for Assessing Technology Transfer Vectors and Vulnerabilities

In pursuit of global talent, the Chinese government creates or sponsors professional associations for experts in scientific and technical industries worldwide.<sup>96</sup> These professional associations vary in scope and mission: Whereas many are purely fraternal social organizations, others are explicitly dedicated to bringing foreign industry knowledge, technology, and talent to China.<sup>97</sup>

To find the total number of Chinese professional associations operating in each country, we conducted systematized Google and Baidu searches using generic Mandarin-language phrases such as “Chinese-German Technology Cooperation Association” (中德技术合作协会). Many of the organizations are constituents of larger “federations” (会联合会) of Chinese professional associations, which list the names of all their members. We compiled the names and websites of all associations affiliated with the European and world federations, in addition to results from manual searches, to produce the figures in this report. These findings are preliminary; additional professional associations may operate in each country. In future research, we plan to disambiguate between organizations explicitly involved in technology transfer and those that engage in purely legal, benign activities.<sup>98</sup>



## Appendix III. Multilateral Fora for AI Cooperation

### FIVE EYES

Organization Profile: Five Eyes is an intelligence designation between the United States, Canada, United Kingdom, Australia, and New Zealand used for information sharing and joint operations. In 2018, media reports claimed the Five Eyes began exchanging information with “like-minded” countries, such as Japan and Germany, in response to concerns about Chinese technology transfer programs.<sup>99</sup>

Current Work Related to AI: Limited public information on this alliance and their respective agencies makes it difficult to assess the extent to which Five Eyes collaborate on AI.

- Five Eyes countries collaborate with Germany, France, and Japan to counter China’s influence and exchange information related to sensitive technology transfers to China.<sup>100</sup>
- Five Eyes countries run the Technical Cooperation Program (TTCP), which is a forum for defense science and technology collaboration. The forum provides a platform for member states to familiarize themselves with each other’s programs, identify common areas of interest and existing gaps, opportunities for joint research, transfer of materials, and general data and information sharing.<sup>101</sup>
- The United Kingdom allegedly tested an autonomous video feed system for battlefield effectiveness in Canada through Five Eyes collaboration.<sup>102</sup>

Comparative Advantages of Five Eyes: Five Eyes is a collaborative intelligence network of like-minded countries. Members have built a substantial amount of trust through this alliance and actively share data to support intelligence needs.<sup>103</sup> Collectively, Five Eyes members have a significant amount of resources available to support the following initiatives to:

- Prevent the transfer of sensitive technical information;
- Coordinate investment screening procedures;
- Share, pool, and store non-sensitive data sets;
- Invest in privacy-preserving machine learning;
- Launch AI R&D collaboration challenge; and
- Promote interoperability and agile software development.

### ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD)

Organization Profile: OECD is a 36-member intergovernmental economic body and UN observer agency. This forum is committed to promoting democratic and market economy values and enables member states to establish best practices, discuss solutions to common problems, express concerns, and coordinate policies.<sup>104</sup>

Current Work Related to AI: The OECD promotes responsible practices for AI development and fosters trust between member states to improve collaboration and best practices. The forum seeks to protect human rights, democratic values, privacy, and digital security.<sup>105</sup> OECD aims to focus on both developed and developing countries.

- OECD's AI expert group called "AIGO" established AI principles and recommendations.<sup>106</sup>
- OECD established the first intergovernmental standards on AI after adopting the "Principles on Artificial Intelligence" in May 2019.<sup>107</sup>
- OECD will implement its recommendations through the AI Policy Observatory, to be launched in early 2020.<sup>108</sup> The observatory will work with OECD, partner countries, NGOs, international organizations, and private sector entities on AI policy across a range of sectors and industries.<sup>109</sup> The policy observatory will evaluate national strategies and measure AI trends and progress.<sup>110</sup>
- The "Going Digital" project aims to formulate policies and strategies for digital development, market openness, greater connectivity, transparency, privacy, and trust to advance digital economies in developing countries.<sup>111</sup>

Comparative Advantages of OECD: The OECD's commitment to democratic principles, responsible AI development, and transparency is advantageous for building trust and establishing norms. Member countries have coordinated trade and economic policies through the OECD.<sup>112</sup> The forum could support the following initiatives to:

- Share, pool, and store non-sensitive data sets;
- Invest in privacy-preserving machine learning;
- Launch AI R&D collaboration challenge;
- Shape norms and standards for AI; and
- Establish a multilateral digital infrastructure network.

## **INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS (ICDPPC)**

Organization Profile: The ICDPPC is an international forum and conference focused on data protection, privacy, and freedom of information.<sup>113</sup> The forum involves governmental agencies and international organizations across the globe. While the ICDPPC focuses on data privacy, the organization aims to promote discussion, information sharing, and cooperation. The ICDPPC hosts primarily closed sessions for members to vote on declarations and resolutions. The ICDPPC has binding agreements, and members are required to provide a point of contact to furnish information on the implementation of resolutions and declarations.<sup>114</sup> The ICDPPC occasionally holds enforcement cooperation meetings.<sup>115</sup>

Current Work Related to AI: In 2018, the ICDPPC put AI on the agenda of its conferences. Since most conference meetings are closed, it is unclear the extent to which ICDPPC members have collaborated on AI.

- In 2018, the ICDPPC adopted the "Declaration on Ethics and Data Protection in Artificial Intelligence."<sup>116</sup> The declaration focuses on ethics, accountability, transparency, privacy, human rights, and the risk of bias and discrimination.
- In 2017, the ICDPPC adopted the "Resolution on Data Protection in Automated and Connected

Vehicles.” The resolution focuses on data privacy, protection, and security for automated and connected vehicles.<sup>117</sup>

- The ICDPPC has a working group on Ethics and Data Protection in Artificial Intelligence.

Comparative Advantages of the ICDPPC: The ICDPPC’s oversight mechanisms could prove beneficial to ensure accountability. The ICDPPC could be particularly valuable for supporting the following initiatives to:

- Share, pool, and store non-sensitive data sets;
- Invest in privacy-preserving machine learning; and
- Shape norms and standards for AI.

## MULTILATERAL ACTION ON SENSITIVE TECHNOLOGIES (MAST) CONFERENCE

Organization Profile: The U.S. State Department convenes the MAST forum to bring together 15 “like-minded” countries to counter China’s influence, exchange and compare information, and respond to China’s efforts to acquire sensitive technology.<sup>118</sup> The conference began in 2018 and seeks to build a “coalition of caution” to curb Chinese acquisition of sensitive technology. The United States claims that MAST interactions have provided information about China’s attempts to exploit the U.S. educational system.<sup>119</sup>

Current Work Related to AI: There is little publicly available information on MAST and its current work. Furthermore, public opening statements from a MAST conference do not specifically mention AI.<sup>120</sup> Nonetheless, the U.S. Department of State has stated that interactions through MAST have informed U.S. export controls, investment reviews, and visa screenings.

Comparative Advantages of MAST: MAST is a narrowly focused forum that can inform participants on methods for sensitive technology transfers and help formulate responses. Should the MAST conference continue, the forum could be used to support the following U.S. AI initiatives to:

- Prevent the transfer of sensitive technical information; and
- Coordinate investment screening procedures.

## WORLD SEMICONDUCTOR COUNCIL (WSC)

Organization Profile: The World Semiconductor Council is an international forum that brings together semiconductor industry associations from the United States, Europe, Japan, South Korea, Taiwan, and China.<sup>121</sup> The organization is based on a set of principles promoting industry cooperation, growth, and fair market trade. The WSC forum emphasizes four main issue areas: environment, safety, and health; intellectual property rights; free and open markets; and market trends.<sup>122</sup>

Current Work Related to AI: The WSC provides recommendations, principles, statements, and white papers for its four main issues. WSC conducts government/authorities meetings on semiconductors (GAMS) to discuss industry policies.<sup>123</sup> WSC activities respect World Trade Organization (WTO) rules and the domestic laws of each respective member.<sup>124</sup>

Comparative Advantages of the World Semiconductor Council: The WSC relies on a flexible approach and consideration for the domestic laws of its members. WSC’s membership includes a range of semiconductor associations, and the forum could support the following U.S. AI initiatives to:

- Coordinate investment screening procedures; and
- Exploit hardware chokepoints.

## SEMICONDUCTOR EQUIPMENT AND MATERIALS INTERNATIONAL (SEMI)

Organization Profile: SEMI is a global association for the semiconductor industry and related technology. SEMI organizes conferences, technology showcases, and meetings to discuss and develop industry standards.<sup>125</sup>

Current Work Related to AI: SEMI has created various industry standards for the respective technology groups it covers. In addition, SEMI has produced a wide range of articles and presentations on U.S.-China relations pertaining to semiconductor market trends.<sup>126</sup>

- In July 2017, SEMI hosted a forum, produced a report, and published other material covering China's integrated circuit manufacturing.<sup>127</sup>
- In October 2019, SEMI released the heterogeneous integration roadmap (HIR) for R&D collaboration.<sup>128</sup>

Comparative Advantages of SEMI: SEMI brings together more than 2,000 members from a range of technology groups, including electronics design, electronics materials, semiconductor manufacturing, sensors and micro-electromechanical systems (MEMS), advanced packaging, and flexible electronics.<sup>129</sup> The range and quantity of industry members is particularly valuable for the following initiatives to:

- Exploit hardware chokepoints;
- Launch AI R&D Collaboration Challenge;
- Develop inter-allied human capital initiative for AI; and
- Shape norms and standards for AI.

## WORLD ECONOMIC FORUM

Organization Profile: The World Economic Forum is an international forum for public-private partnerships and world leaders. The forum meets annually to bring together global entities and convenes six to eight times a year regionally.<sup>130</sup>

Current Work Related to AI: The World Economic Forum has published several articles on its website covering topics related to AI.

- In 2014, the forum produced a report "Delivering Digital Infrastructure Advancing the Internet Economy," which discusses the consequences of digital infrastructure projects and encourages investments.<sup>131</sup>
- In 2019, the forum's annual meeting focused on "Globalization 4.0: shaping a global architecture in the age of the fourth industrial revolution," which discussed principles for artificial intelligence.
- In May 2019, the World Economic Forum collaborated with different organizations to convene a workshop and produce a report on children and AI.<sup>132</sup>

Comparative Advantages of the World Economic Forum: The World Economic Forum serves as a platform for governments and businesses to set priorities, determine investment opportunities, and develop opportunities for investments. The forum could be particularly useful to support the following initiatives to:

- Shape norms and standards for AI; and
- Establish a multilateral digital infrastructure network.

## INTERNATIONAL TELECOMMUNICATION UNION (ITU)

Organization Profile: The ITU is a UN body that governs international telecommunications. It helps to evaluate and develop telecommunication standards, address ongoing challenges, and improve connectivity in the developing world. The ITU hosts conferences that bring together stakeholders on a global and regional basis to discuss information and communication technology (ICT).<sup>133</sup>

Current Work Related to AI: The ITU has developed several initiatives related to AI.

- In 2017, the ITU established the Focus Group on Machine Learning for Future Networks 5G (FG-ML5G), which creates technical reports on machine learning for future networks.<sup>134</sup>
- In 2018, the ITU established the Focus Group on Artificial Intelligence for Health (FG-AI4H), which collaborates with the World Health Organization (WHO) and works to create a framework to evaluate AI-driven health technology.<sup>135</sup>
- The ITU has hosted the AI for Good series since 2017, which brings together industry stakeholders to discuss ethical, technical, and societal issues on AI. This forum intends to establish guidelines, recommendations, and foster cooperation for AI innovation.<sup>136</sup>

Comparative Advantages of the ITU: The ITU has been active in researching and promoting debate on AI and has an expansive membership of 193 countries and 900 members from companies, universities, and international organizations.<sup>137</sup> The organization could support the following initiatives to:

- Shape global norms and standards for AI; and
- Establish a multilateral digital infrastructure network.<sup>138</sup>

## G20

Organization Profile: The G20 is an international forum comprising the world's 20 largest economies, which together encompass approximately 80 percent of global GDP. The summit brings together national leaders and banking institutions to discuss and coordinate economic policy.<sup>139</sup>

Current Work Related to AI: Leaders discussed AI during the 2019 G20 Summit in Osaka and as a result:

- Established non-binding guiding principles on AI in June 2019.<sup>140</sup>
- Issued the Osaka Declaration to promote the notion of "data free flow with trust" and "interoperability of different frameworks."<sup>141</sup>

Comparative Advantages of the G20: The G20 promotes trust, interoperability, and data sharing among members. Policymakers could use this forum to:

- Share, pool, and store non-sensitive data sets;
- Invest in privacy-preserving machine learning; and
- Shape global norms and standards for AI.

## ASIAN DEVELOPMENT BANK (ADB)

Organization Profile: The Asian Development Bank is a regional banking institution focused on reducing poverty and promoting development in Asia and the Pacific.<sup>142</sup>

Current Work Related to AI: The Asian Development Bank promotes several initiatives to support digital infrastructure in Asia.

- In 2019, the ADB released the Digital Agenda Strategy 2030, which aims to transform the region digitally by improving and augmenting information and communication technology and promoting interconnectedness and greater data access. ADB committed \$118.3 million for the first stage of this project.<sup>143</sup> The ADB's Digital Agenda Strategy 2030 outlines a roadmap and timeline for investments and infrastructure development.
- From 2010 to 2018, ADB supported 315 projects focused on digital education in the healthcare sector, smart phone finance tools, digital identity systems, smart grids for renewable energy, smart sensors for non-revenue water reductions, and traffic control.<sup>144</sup>

Comparative Advantages of the Asian Development Bank: ADB's efforts to fund regional digital infrastructure could support the following initiatives to:

- Share, pool, and store non-sensitive data sets;
- Invest in privacy-preserving machine learning; and
- Establish a multilateral digital infrastructure network.

## INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

Organization Profile: The ISO is an international body that sets standards for various products and technologies.<sup>145</sup>

Current Work Related to AI: ISO has established international standards for some AI technologies. The organization also collaborates with the International Electrotechnical Commission (IEC) to establish guidelines and ensure that intellectual property rights are protected.

- ISO-IEC joint technical committee (JTC1) reviews and sets standards for various information technologies (IT). JTC1 works on standards, AI safety and trustworthiness, AI industry applications, and big data.<sup>146</sup>
- JTC1 has two subcommittees, including SC 41 on the Internet of Things (IoT) and SC 42 on AI.<sup>147</sup>
- ISO has three published standards for AI and thirteen in progress.<sup>148</sup>

Comparative Advantages of ISO: The ISO is a leading international standards body with members from 164 countries. ISO's global reach, in addition to the organization's efforts to establish standards for AI technologies, could support the following U.S. AI initiatives to:

- Share, pool, and store non-sensitive data sets;
- Invest in privacy-preserving machine learning; and
- Shape global norms and standards for AI.



## WORLD BANK

Organization Profile: The World Bank is an international banking organization that provides loans and grants to assist developing countries.<sup>149</sup>

Current Work Related to AI: The World Bank's primary work related to AI is its investments in digital infrastructure for developing countries.

- The World Bank has a Digital Development Partnership, which fosters public-private partnerships to implement digital development strategies.<sup>150</sup>
- In 2018, the World Bank and the Center for Effective Global Action hosted a one-day workshop at Google focusing on the role of artificial intelligence in tackling economic development challenges.<sup>151</sup>
- The World Bank and the Future Society plan to release a joint policy report called "Policy & Regulatory Pathways to Harness AI in Developing Countries."<sup>152</sup>

Comparative Advantage of the World Bank: The World Bank's efforts to fund global digital infrastructure and development could support the following initiative to:

- Establish a multilateral digital infrastructure network.

## WORLD TRADE ORGANIZATION (WTO)

Organization Profile: The WTO is an intergovernmental agency responsible for regulating international trade. The organization ratifies agreements to promote smooth trade flows, protect intellectual property, and address international trade disputes. The WTO also monitors members to ensure that all parties are transparent and following agreements.<sup>153</sup>

Current Work Related to AI: The WTO has not specifically released any work on AI, but it has been at the forefront of U.S.-China trade issues over sensitive technology transfers.<sup>154</sup>

Comparative Advantages of the WTO: The WTO estimates that its collective membership accounts for at least 96 percent of global trade.<sup>155</sup> The WTO could be useful to address trade disputes and support the following initiatives to:

- Launch an AI R&D Collaboration Challenge; and
- Shape global norms and standards for AI.

## 3RD GENERATION PARTNERSHIP PROJECT (3GPP)

Organization Profile: 3GPP is a standards organization for telecommunications that brings together seven regional telecommunication standards organizations from Europe, Japan, India, China, the United States, and Korea.<sup>156</sup>

Current Work Related to AI: 3GPP has not produced any work specifically related to AI. However, 3GPP has discussed related technologies, including 5G developments and the evolution of the Internet of Things (IoT).<sup>157</sup>

Comparative Advantages of 3GPP: 3GPP sets standards and operates with relative transparency. 3GPP could support the following initiatives to:

- Promote interoperability and agile software development<sup>158</sup>; and
- Shape global norms and standards for AI.

## INTERNATIONAL MONETARY FUND (IMF)

Organization Profile: The IMF is an international organization that promotes financial stability, economic cooperation, and global development. The organization provides oversight for the international economy, distributes loans, and assists countries with economic development.<sup>159</sup>

Current Work Related to AI: The IMF's primary work on AI involves its "fintech" project, which aims to address the challenges and risks associated with implementing emerging technologies in the financial sector.<sup>160</sup>

- In May 2019, the IMF released a policy paper that assesses the state of fintech, identifies areas for international cooperation, and highlights challenges associated with the deployment of emerging financial technology.<sup>161</sup>

Comparative Advantages of the IMF: The IMF's efforts to fund global digital infrastructure could support the following U.S. AI initiatives to:

- Shape global norms and standards for AI; and
- Establish a multilateral digital infrastructure network.

## ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE)

Organization Profile: OSCE is an international security organization focused on human rights, border control, human trafficking, and arms control. OSCE holds conferences and conducts field operations to promote democratic values.<sup>162</sup>

Current Work Related to AI: OSCE has held forums to discuss how artificial intelligence will change law enforcement operations and how criminals may exploit AI for illegal purposes.<sup>163</sup> Most of the OSCE's work has focused on the digital transformation of global economies.

- In 2018, the OSCE held its 25th ministerial meeting, which published decisions and declarations on human capital in the digital era and cooperation in the digital economy. These documents aim to increase collaboration between states, discuss shared challenges, and identify opportunities for public-private partnership.<sup>164</sup>

Comparative Advantages of the OSCE: The OSCE brings together 57 countries committed to promoting democratic values, human rights, and security. In addition, the OSCE facilitates regional and international collaboration among member law enforcement institutions and promotes the use of new technologies to improve police operations.<sup>165</sup> The OSCE's mission and operations could support the following initiatives to:

- Share, pool, and store non-sensitive data sets;
- Invest in privacy-preserving machine learning; and
- Develop inter-allied human capital initiative for AI.

## ASSOCIATION OF SOUTHEAST ASIAN NATIONS (ASEAN)

Organization Profile: ASEAN is a regional intergovernmental organization that aims to promote development, stability, and opportunities for collaboration between members. ASEAN comprises one-fifth of the world's manufacturing industry.<sup>166</sup>

Current Work Related to AI: ASEAN has convened several conferences, dialogues, and committees to discuss how AI will impact regional labor markets and promote digital connectivity.<sup>167</sup>

Comparative Advantage of ASEAN: ASEAN promotes regional collaboration and economic growth. It could support the following initiative to:

- Develop inter-allied human capital for AI.<sup>168</sup>

## DIGITAL 9 (D9)

Organization Profile: Digital 9 is an annual international forum founded in 2014 that includes Canada, Estonia, Israel, United Kingdom, Mexico, New Zealand, Portugal, South Korea, and Uruguay. The forum seeks to bring together countries leading digital developments to share best practices, find opportunities to collaborate, and support digital economic growth for members. Members agree on a set of principles committed to user needs, open standards, open sources, open markets, teaching children to code, government transparency, connectivity, sharing and learning, and citizen access to digital services.<sup>169</sup>

Current Work Related to AI: Digital 9 has four working groups on digital collaboration, artificial intelligence, digital human rights, and Data 360°, which focuses on data management.

- The D9's 2018 Summit in Israel focused on ethical artificial intelligence in which members established the "D9 shared approach for responsible use of AI by governments." This approach emphasizes the importance of transparency, accountability, and procedural fairness.<sup>170</sup>

Comparative Advantages of the D9: D9 members are committed to transparency, cooperation, ethical development, and protecting human rights. Most D9 members have established or expressed interest in creating national data strategies.<sup>171</sup> D9 promotes interoperability, open data, and data sharing, which could support the following initiatives to:

- Share, pool, and store non-sensitive datasets;
- Promote interoperability and agile software development;
- Shape global norms and standards for AI; and
- Establish a multilateral digital infrastructure network.

## WASSENAAR ARRANGEMENT

Organization Profile: The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a global multilateral export regime with 42 participating countries committed to transparency and responsible trade of conventional and dual-use materials. The regime was established in 1996 as a means to exchange information, establish norms and standards, and report on transfers to countries outside of the Wassenaar Arrangement. Participating countries enforce the Wassenaar Arrangement's principles through national legislation and policies. The arrangement aims to prevent rogue actors from acquiring conventional and dual-use technologies. The Wassenaar Arrangement takes decisions by consensus and no single participating country has veto power.<sup>172</sup>

Current Work Related to AI: The Wassenaar Arrangement has not focused on technology related to AI, and neural network integrated circuits are the only technology on the regime's dual-use control list.<sup>173</sup> Since the organization primarily operates with closed-door negotiations, it is possible members have exchanged information on or discussed adding other AI technologies.<sup>174</sup>

- In a 2017 interview, Head of the Wassenaar Arrangement Secretariat, Philip Griffiths, discussed how the Wassenaar Arrangement has been working over the last three years to evaluate and improve their understanding of the impact of emerging technologies such as artificial intelligence.<sup>175</sup>

Comparative Advantages of the Wassenaar Arrangement: This multilateral export regime has promoted transparency and coordination on responsible technology transfers to prevent potentially destabilizing proliferation. The Wassenaar Arrangement export regime and dual-use control lists could support the following initiatives to:

- Exploit hardware chokepoints; and
- Prevent the transfer of sensitive technical information.

## Endnotes

1. On Chinese and Russian efforts to export digital authoritarianism, see Valentin Weber, "The Worldwide Web of Chinese and Russian Information Controls," *Centre for Technology and Global Affairs*, University of Oxford, September 17, 2019; Alina Polyakova and Chris Meserole, "Exporting digital authoritarianism," *Brookings Institution*, August 26, 2019; Kara Frederick, Daniel Kliman, and Ely Ratner, "The Low Road: Charting China's Digital Expansion," *Center for a New American Security*, September 4, 2019; Paul Eckert, "Global Freedom Declines as Chinese, Russian Info Control Practices Spread, Says Study," *Radio Free Asia*, September 17, 2019, <https://www.rfa.org/english/news/china/information-controls-09172019153506.html>.
2. Weber, "The Worldwide Web of Chinese and Russian Information Controls."
3. For additional perspectives, see National Security Commission on Artificial Intelligence, Interim Report, November 2019, <https://drive.google.com/file/d/153OrxnuGEjsUvLxWsFYauslwNeCEkvUb/view>; Martijn Rasser, Megan Lamberth, Ainikki Riikonen, Chelsea Guo, Michael Horowitz, and Paul Scharre, "The American AI Century: A Blueprint for Action," *Center for a New American Security*, December 2019, [https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Tech-American-AI-Century\\_updated.pdf?mtime=20200103081822](https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Tech-American-AI-Century_updated.pdf?mtime=20200103081822).
4. For more on the survey methodology, please refer to Appendix I. For more on the methodology to assess Chinese technology transfer pathways in allied and partner countries, see Appendix II. For a list of multilateral fora, see Appendix III.
5. On the "survival strategies" and durability of authoritarian regimes, see Natasha Lindstaedt, Andrea Kendall-Taylor, and Erica Frantz, *Democracies and Authoritarian Regimes* (Oxford: Oxford University Press, 2020).
6. Sino-Russian cooperation is strengthening across a number of areas. See Alexander Gabuev, "How China Became Russia's Most Important Partner," *Carnegie Moscow Center*, September 29, 2019, <https://carnegie.ru/2019/09/29/how-china-became-russia-s-most-important-partner-pub-79948>; Elsa B. Kania and Samuel Bendett, "A new Sino-Russian high-tech partnership," *Australian Strategic Policy Institute*, October 29, 2019, <https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership>.
7. See, e.g., Weber, "The Worldwide Web of Chinese and Russian Information Controls."
8. See, e.g., Lora Saalman, "The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Volume II," *SIPRI*, October 2019, <https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-ii>; Michael C. Horowitz, Paul Scharre, and Alexander Velez-Green, "A Stable Nuclear Future? The Pact of Autonomous Systems and Artificial Intelligence," *arXiv*, December 11, 2019, <https://arxiv.org/abs/1912.05291>.
9. Miles Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Preventing, and Mitigation," February 2018, <https://arxiv.org/pdf/1802.07228.pdf>.
10. See, e.g., Paul Scharre and Michael Horowitz, "Artificial Intelligence: What Every Policymaker Needs to Know," *Center for a New American Security*, June 19, 2018. On the trade-offs between capability and

vulnerability in the cyber domain, see Jacquelyn Schneider, "The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war," *Journal of Strategic Studies* 42, Issue 6 (2019): 841-863.

11. On the link between international collaboration and quality of research, see "Artificial Intelligence: How knowledge is created, transferred, and used," *Elsevier*, December 11, 2018, <https://p.widencdn.net/jj2lej/ACAD-RI-AS-RE-ai-report-WEB>.

12. See, e.g., Anne-Marie Slaughter, "America's Edge," *Foreign Affairs*, January/February 2009, <https://www.foreignaffairs.com/articles/united-states/2009-01-01/americas-edge>.

13. See, e.g., Stephen D. Krasner (ed.), *International Regimes* (Ithaca: Cornell University Press, 1983); Lisa L. Martin and Beth A. Simmons, "International Organizations and Institutions," in Walter Carlsnaes, Thomas Risse, Beth A. Simmons, *Handbook of International Relations* (Thousand Oaks, CA: Sage Publications, 2002), 192-211.

14. Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, Issue 1 (Summer 2019): 42-79.

15. *Ibid.*

16. "Russia Says BRICS Nations Favor Idea of Common Payment System," *The Moscow Times*, November 17, 2019, <https://www.themoscowtimes.com/2019/11/14/putin-to-invite-china-and-india-to-join-anti-sanctions-bank-network-a68172>.

17. On securing America's defense innovation base through alliances, see Daniel Kliman, *Center for a New American Security*, ongoing research.

18. When asked about obstacles to collaboration with the United States in the CSET survey, for example, multiple officials highlighted industrial competition as an obstacle. On international competition for talent, see Remco Zwetsloot, James Dunham, Zachary Arnold, and Tina Huang, "Keeping Top Talent in the United States: Findings and Policy Options for International Graduate Student Retention," *Center for Security and Emerging Technology*, <https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf>; "Technology and Geopolitics: Navigating a Future of Tech Uncertainty," *Asia Pacific Foundation of Canada*, Conference Report, [https://www.asiapacific.ca/sites/default/files/apf\\_canada\\_technology\\_and\\_geopolitics\\_conference\\_report.pdf](https://www.asiapacific.ca/sites/default/files/apf_canada_technology_and_geopolitics_conference_report.pdf); Celia Chen, "Trade war turning Chinese students off the US, with many opting for UK, Canada and Australia, says payments firm," *South China Morning Post*, May 28, 2019.

19. See, e.g., Kenneth Neil Cukier, "Ready for Robots?" *Foreign Affairs* July/August 2019.

20. Andrew Imbrie and Elsa B. Kania, "AI Safety, Security, and Stability Among Great Powers: Options, Challenges, and Lessons Learned for Pragmatic Engagement," *Center for Security and Emerging Technology*, December 2019.

21. *Ibid.*

22. See, e.g., Tim Dutton, "An Overview of National AI Strategies," June 28, 2018, <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd>; Tim Dutton, Brent Barron, and Gag Boskovic, "Building an AI World: Report on National and Regional AI Strategies," *CIFAR*, [https://www.cifar.ca/docs/default-source/ai-society/buildinganaiworld\\_eng.pdf](https://www.cifar.ca/docs/default-source/ai-society/buildinganaiworld_eng.pdf); Thomas A. Campbell, "Artificial Intelligence: An Overview of State Initiatives," [http://www.unicri.it/in\\_focus/files/Report\\_AI-An\\_Overview\\_of\\_State\\_Initiatives\\_FutureGrasp\\_7-23-19.pdf](http://www.unicri.it/in_focus/files/Report_AI-An_Overview_of_State_Initiatives_FutureGrasp_7-23-19.pdf).

23. "Artificial Intelligence Benchmark," *Capgemini Consulting*, <https://www.capgemini.com/wp-content/uploads/2018/07/AI-Readiness-Benchmark-POV.pdf>.

24. "BSA Global Cloud Computing Country Checklist," BSA, [https://cloudscorecard.bsa.org/2016/pdf/BSA\\_2016\\_Global\\_Cloud\\_Scorecard\\_TABLE.pdf](https://cloudscorecard.bsa.org/2016/pdf/BSA_2016_Global_Cloud_Scorecard_TABLE.pdf). See also "DATA Protection Laws of the World," DLA Piper, <https://www.dlapiperdataprotection.com/index.html?t=authority&c=DE>.
25. For a list of U.S. allies and partners, we referred to U.S. Department of State fact sheets and designations. For a list of countries with AI strategies and investments, see Campbell, "Artificial Intelligence: An Overview of State Initiatives." Due to resource and time constraints, we could not include every U.S. ally and partner that has put effort into developing a national strategy or made significant investments in AI. Though we recognize their importance, our analysis does not include some U.S. allies and partners, including Hungary, Malta, South Africa, and Tunisia.
26. Our final case list comprises Australia, Austria, Brazil, Canada, Chile, Colombia, Czech Republic, Denmark, Estonia, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Latvia, Lithuania, Malaysia, Mexico, the Netherlands, New Zealand, the Philippines, Poland, Qatar, Saudi Arabia, Singapore, South Korea, Spain, Sweden, Taiwan, the United Arab Emirates, and the United Kingdom. We include the United States, China, and Hong Kong for comparison.
27. Survey results do not include Brazil, China, Hong Kong, Kenya, the Philippines, Poland, Qatar, Saudi Arabia, Taiwan, the United Arab Emirates, or the United States.
28. William Hannas and Huey-meei Chang, "China's Access to Foreign AI Technology: An Assessment," *Center for Security and Emerging Technology*, Georgetown University, September 2019, [https://cset.georgetown.edu/wp-content/uploads/CSET\\_China\\_Access\\_To\\_Foreign\\_Technology.pdf](https://cset.georgetown.edu/wp-content/uploads/CSET_China_Access_To_Foreign_Technology.pdf).
29. Ibid.
30. Only one official from Colombia confirmed there are no policies in place to counter tech transfer. The remaining third of officials indicated they do not know whether such policies are in place.
31. Experts from the Center for a New American Security recommend that "Congress should increase funding for efforts supporting cyber defense at smaller firms active in critical technology areas." For more information, see Rasser, et al., "The American AI Century," 20-21.
32. Hannas and Chang, "China's Access to Foreign AI Technology."
33. "Dimensions: Publications," *Digital Science*, 2019, <https://app.dimensions.ai/>. LinkedIn may be a poor indicator of global AI talent due to English language restrictions and market penetration challenges, but Element AI's Global AI Talent Report remains one of the most prevalent and methodologically sound approaches to measuring AI experts. See, e.g., JF Gagne, "Some observations on the worldwide AI talent pool in 2019," <https://jfgagne.ai/blog/ai-talent-2019/>.
34. "Global Flow of Tertiary-Level Students," UNESCO, 2017, <http://uis.unesco.org/en/uis-student-flow>. UNESCO data captures the total number of Chinese students—undergraduate, graduate, and doctoral—studying in other countries. However, almost no prominent cases of technology transfer occur via undergraduate students; graduate students and postdoctoral scholars are responsible for the bulk of academic technology transfer. The Chinese government constructs or sponsors professional associations for experts in scientific and technical industries to facilitate informal technology transfer from several countries. Not all professional associations are complicit, but many explicitly aim to incorporate foreign scientists and trade secrets into Chinese firms. See, e.g., Bill Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (London: Routledge, 2018). As an estimate for how many organizations operate in each country, we conducted systematized Mandarin-language keyword searches in Baidu and Google. We tallied the number of groups that are constituents of world and regional "federations" of Chinese professional associations. For more information, see Appendix II.



35. According to the FBI, "The vast majority of students and researchers from China are in the United States for legitimate academic reasons and contribute to the diversity of backgrounds and ideas important in our society." See "China: The Risk to Academia," Federal Bureau of Investigation, June 2019, <https://www.fbi.gov/file-repository/china-risk-to-academia-2019.pdf/view>.
36. "1000 Talents Plan," State Council of the People's Republic of China, 2010, <http://www.1000plan.org.cn/en/>.
37. "Overseas Offices," Federal Bureau of Investigation, 2019, <https://www.fbi.gov/contact-us/legal-attache-offices>.
38. Based on the CSET survey, officials from Australia, Colombia, the Czech Republic, Italy, Lithuania, and the EU were interested in collaborating on investment screening procedures with the United States. See also Hannas and Chang, "China's Access to Foreign AI Technology."
39. "China Global Investment Tracker," *American Enterprise Institute*, 2019, <https://www.aei.org/china-global-investment-tracker/>.
40. "FDI inflows, by region and economy, 1990-2018," *United Nations Conference on Trade and Development*, June 12, 2019, <https://unctad.org/en/Pages/DIAE/World%20Investment%20Report/Annex-Tables.aspx>.
41. "Membership of Nonproliferation Export Control Regimes, HCOC and PSI," *Nuclear Threat Initiative*, October 26, 2015, [https://media.nti.org/documents/apmnecr\\_sCQhT3r.pdf](https://media.nti.org/documents/apmnecr_sCQhT3r.pdf).
42. Thilo Hanemann, Mikko Huotari, and Agatha Kratz, "Chinese FDI in Europe: 2018 Trends and Impact of New Screening Policies," *Rhodium Group*, March 6, 2019, <https://rhg.com/research/chinese-fdi-in-europe-2018-trends-and-impact-of-new-screening-policies/>.
43. Catherine Wong, "Why Greece is banking on China's modern-day Silk Road to help its economic recovery," *South China Morning Post*, December 26, 2017, <https://www.scmp.com/news/china/diplomacy-defence/article/2125506/why-greece-banking-chinas-modern-day-silk-road-help-its>.
44. "China Trade Summary 2017 Data," *World Integrated Trade Solution*, *World Bank*, 2018, <https://wits.worldbank.org/CountryProfile/en/Country/CHN/Year/2017/Summary>.
45. SEMI, *World Fab Forecast*, May 2019 edition.
46. Saif M. Khan, "Maintaining the AI Chip Competitive Advantage of the United States and its Allies," *Center for Security and Emerging Technology*, December 2019, <https://cset.georgetown.edu/wp-content/uploads/CSET-Maintaining-the-AI-Chip-Competitive-Advantage-of-the-United-States-and-its-Allies-20191206.pdf>.
47. Our survey asked officials whether their country was considering increased regulations around the import/export of semiconductor manufacturing equipment. While half of officials were not sure, five considered such action to be unlikely. Two (Italy and South Korea) considered such actions somewhat likely.
48. We include figures for integrated circuit and logic production capacity, generated from SEMI, *World Fab Forecast*, May 2019 edition.
49. "Integrated Circuits," *Observatory of Economic Complexity*, 2019, <https://oec.world/en/profile/hs92/847193/>. Based on data from the UN Conference on Trade and Development.
50. Saif M. Khan, "Maintaining the AI Chip Competitive Advantage of the United States and its Allies."
51. Quality-adjusted IC logic capacity is equivalent to the number of transistors manufactured on wafers per month.



52. Shang-su Wu, "Undersea Surveillance: Supplementing the ASEAN Indo-Pacific Outlook," *Center for International Maritime Security*, September 3, 2019.
53. Mark Newton, Rachel Rizzo, Julianne Smith, and Jim Townsend, "More Than Burden Sharing: Five Objectives for the 2018 NATO Summit," *Center for a New American Security*, June 18, 2018, <https://s3.amazonaws.com/files.cnas.org/documents/NATO-Report-FINAL.pdf?mtime=20180619140623>.
54. CSET survey results indicate that the EU, Colombia, Lithuania, the United Kingdom, Japan, Australia, Italy, France, Chile, and South Korea are taking action to create data use standards, archival procedures, or both. On the importance of promoting common data standards and the challenges of accessing clean and usable data, see Michael Stumborg, "See You in a Month: AI's Long Data Tail," *War on the Rocks*, October 17, 2019.
55. "Open Data," Open Government Initiative, *The White House*, May 2013, <https://obamawhitehouse.archives.gov/open>.
56. Global Open Data Index, "Place overview," 2019, <https://index.okfn.org/place/>.
57. "Colocation Data Centers," *Cloudscene*, October 2019, <https://cloudscene.com/browse/data-centers>; Alexander Simoes, "Computer Data Storage Units," *Observatory of Economic Complexity*, 2019, <https://oec.world/en/profile/hs92/847193/>. Based on data from the UN Conference on Trade and Development.
58. "Data Protection Laws of the World," *DLA Piper Intelligence*, 2019, <https://www.dlapiperdataprotection.com/>.
59. Signed in 2018, the General Data Protection Regulation is the European Union's comprehensive data protection law, regulating how companies collect, access, and transmit data across borders. For more information, see "What is GDPR? Everything you need to know, from requirements to fines," *IT Pro*, December 23, 2019, <https://www.itpro.co.uk/it-legislation/27814/what-is-gdpr-everything-you-need-to-know>.
60. Helen Toner and Roxanne Heston, "Have Your Data and Use it Too: A Federal Initiative for Protecting Privacy while Advancing AI," *Day One Project*, January 23, 2020, <https://www.dayoneproject.org/protectingprivacyintheaiera>, 5.
61. For more on these and other examples of privacy-preserving machine learning, see Erica Portnow, Gennie Gebhart, and Starchy Grant, "Facial Recognition, Differential Privacy, and Trade-Offs in Apple's Latest OS Releases," *Electric Frontier Foundation*, September 27, 2016; "Secure multi-party computation considered for fighting VAT fraud in Estonia," *Estonia Cyber Security News Aggregator*, January 29, 2015; Peeter Laud and Liina Kamm, *Applications of Secure Multiparty Computation* (Amsterdam: IOS Press, 2015); John M. Abowd, "Why the Census Bureau Adopted Differential Privacy for the 2020 Census of Population," *Harvard University Privacy Tools Project*, accessed December 2019.
62. "AI Ethics Principles," Australian Government, Department of Industry, Innovation, and Science, <https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles>.
63. Ibid.
64. "Dimensions: Publications," *Digital Science*, 2019, <https://app.dimensions.ai/>.
65. Adrian Shahbaz, "The Rise of Digital Authoritarianism: Freedom on the Net 2018," *Freedom House*, November 1, 2018, [https://freedomhouse.org/sites/default/files/FOTN\\_2018\\_Final%20Booklet\\_11\\_1\\_2018.pdf](https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf); Bhaskar Chakravorti, "Why Digital Trust is So Different Around the World," *OECD Forum Network*, February 19, 2018, <https://www.oecd-forum.org/users/79580-bhaskar-chakravorti/posts/30470-why-digital-trust-is-so-different-around-the-world>; "2019 CIGI-Ipsos

Global Survey on Internet Security and Trust," *Centre for International Governance Innovation*, June 11, 2019, [https://www.ipsos.com/sites/default/files/ct/news/documents/2019-06/cigi-ipsos-2019-dt-6-11-2019\\_0.pdf](https://www.ipsos.com/sites/default/files/ct/news/documents/2019-06/cigi-ipsos-2019-dt-6-11-2019_0.pdf).

66. For discussions about the importance of interoperability and shared data standards, see Ryan Schultz, Karla Keelean, James Jamison, and Ralph O'Connell, "Data Sharing is a Critical Capability," *MODSIM World*, Paper no. 28, 2017, 1-12, [https://www.modsimworld.org/papers/2017/Data\\_Sharing\\_is\\_a\\_Critical\\_Capability.pdf](https://www.modsimworld.org/papers/2017/Data_Sharing_is_a_Critical_Capability.pdf); James Tolbert, "Harmonizing Interoperability," *The Three Swords Magazine*, no. 30, 2016, 56-57, [https://www.jwc.nato.int/images/stories/\\_news\\_items\\_/2016/Harmonizing\\_Interoperability.pdf](https://www.jwc.nato.int/images/stories/_news_items_/2016/Harmonizing_Interoperability.pdf).

67. Danielle C. Tarraf, "Our Future Lies in Making AI Robust and Verifiable," *War on the Rocks*, October 22, 2019.

68. Jasmin Léveillé, "Embrace Open-Source Military Research to Win the AI Competition," *War on the Rocks*, October 16, 2019.

69. "Welcome to the AI4EU Platform," European Union Horizon 2020 Research and Innovation Program, 2019, <https://www.ai4eu.eu/>.

70. Indicators included the number of military bases in each country owned and operated by U.S. service branches, "Bases Around the World," *Today's Military*, January 2020, <https://www.todayismilitary.com/about-military/bases-around-world>; troop contributions to ongoing NATO operations, including Kosovo Force (KFOR), International Security Assistance Force (ISAF), and Operation Sea Guardian; trade registers generated from "SIPRI Arms Transfers Database," *Stockholm International Peace Research Institute*, capturing years 2016-2019, <https://sipri.org/databases/armstransfers>; and "U.S. Collective Defense Arrangements," U.S. Department of State, 2017, <https://2009-2017.state.gov/s/l/treaty/collectivedefense//index.htm>.

71. See "Major Non-NATO Ally," *Global Security*, 2017, <https://www.globalsecurity.org/military/agency/dod/mnna.htm>; "Membership of Nonproliferation Export Control Regimes, HCOC and PSI," *Nuclear Threat Initiative*, 2019, [https://media.nti.org/documents/apmneqr\\_sCQhT3r.pdf](https://media.nti.org/documents/apmneqr_sCQhT3r.pdf); "Partners," *The Global Coalition Against Daesh*, 2019, <https://theglobalcoalition.org/en/partners/>; "Members and Partners," *The Global Counterterrorism Forum*, 2019, <https://www.thegctf.org/About-us/Members-and-partners>.

72. "Defense Primer: The National Technology and Industrial Base," *Congressional Research Service*, September 17, 2019, <https://crsreports.congress.gov/product/pdf/IF/IF11311>.

73. DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," U.S. Department of Defense, May 5, 2004, <https://biotech.law.lsu.edu/blaw/dodd/corres/pdf2/d46305p.pdf>.

74. Authors' calculations, across all fields, based on numbers from the OECD. We include total R&D investment because many of the professors that governments fund with federal dollars also work at private companies, and the direction of the AI field is heavily influenced by industry R&D funding, including in the physical sciences.

75. Tarraf, "Our Future Lies in Making AI Robust and Reliable."

76. Nineteen of twenty-eight EU member states have formed a consortium to support the development of eight supercomputing centers throughout the EU. For more information, see "Digital Single Market: Europe announces eight sites to host world-class supercomputers," European Commission, June 6, 2019, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_2868](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2868).

77. "2018 Global R&D Funding Forecast," *R&D Magazine*, November 16, 2017, <https://abm-website-assets.s3.amazonaws.com/rdmag.com/s3fs-public/Tim%20Studt%20GS%203%20GFF.pdf>; "Business Enterprise Expenditure by Industry," *OECD Digital Economy Outlook*, 2017, [https://stats.oecd.org/Index.aspx?DataSetCode=BERD\\_IND](https://stats.oecd.org/Index.aspx?DataSetCode=BERD_IND).
78. "Connected World: Patterns of International Collaboration Captured by the Nature Index, 2018-2019," *Nature Index*, 2019, <https://www.natureindex.com/faq>.
79. The Nature Index collaboration score measures countries' and institutions' aggregate contributions to articles in leading scientific journals over a specific time frame. For more information about how scores are calculated, see "A guide to the Nature Index," *Nature*, June 27, 2018, <https://www.nature.com/articles/d41586-018-05559-2>.
80. "Partnerships for International Research and Education (PIRE)," *National Science Foundation*, 2016, <https://www.nsf.gov/pubs/2016/nsf16571/nsf16571.htm>; "Meet the Partners," *Partnership on AI*, October 30, 2019, <https://www.partnershiponai.org/partners/>.
81. "The Roots of Innovation: U.S. Chamber International IP Index," *U.S. Chamber of Commerce*, no. 5 (2017): ii-iii, [http://www.theglobalipcenter.com/wp-content/uploads/2017/02/GIPC\\_IP\\_Index\\_2017\\_Report.pdf](http://www.theglobalipcenter.com/wp-content/uploads/2017/02/GIPC_IP_Index_2017_Report.pdf).
82. "International Property Rights Index: Countries," *Property Rights Alliance*, 2019, <https://www.internationalpropertyrightsindex.org/countries>.
83. "Patent publications by applicant origin, 2018," *World Intellectual Property Organization*, October 2019, <https://www3.wipo.int/ipstats/>.
84. "Building the Future: Investing in Discovery and Innovation: NSF Strategic Plan for Fiscal Year (FY) 2018-2022," *National Science Foundation*, February 2018. For a specific example, see NSF 20-013, "Dear Colleague Letter: 2020 CHE International Supplement," <https://www.nsf.gov/pubs/2020/nsf20013/nsf20013.jsp>.
85. JF Gagne, Grace Kiser, and Yoan Mantha, "Global AI Talent Report 2019," *Element AI*, 2019, <https://jfgagne.ai/talent-2019/>.
86. We estimate the number of outbound, internationally mobile college graduates with STEM and ICT degrees by multiplying figures from "Education: Net flow ratio of outbound internationally mobile students," as well as "Education: Percentage of graduates from tertiary education graduating from Information and Communication Technologies programmes," and "Education: Percentage of graduates from Science, Technology, Engineering, and Mathematics programmes in tertiary education, both sexes," found in "Data for the Sustainable Development Goals," *United Nations Educational, Scientific and Cultural Organization*, 2019, <http://data.uis.unesco.org/>.
87. The Department of Defense's trusted capital marketplace is one form that such a common market could take in the defense sector. See Yasmin Tadjdeh, "News from AUVSI Defense: Wary of China, Pentagon to Launch 'Trusted Capital Marketplace' This Fall," *National Defense*, August 8, 2019. Peter Spiegel and Andrew Edgecliffe-Johnson, "US navy secretary warns of fragile supply chain," *Financial Times*, November 5, 2019.
88. "8th pillar: Government usage," *World Economic Forum*, Networked Readiness Index, Global Information Technology Report, 2016, <http://reports.weforum.org/global-information-technology-report-2016/networked-readiness-index/>; "Mapping AI Governance," *Nesta*, 2019, <https://www.nesta.org.uk/data-visualisation-and-interactive/mapping-ai-governance/>.
89. "Global Diplomacy Index," *Lowy Institute*, 2017, <https://globaldiplomacyindex.lowyinstitute.org/>;

"The Soft Power 30," Portland, FACEBOOK, and USC Center on Public Diplomacy, 2019, <https://softpower30.com/>.

90. In the CSET survey, we asked officials if there is any discussion in their country around increased regulation of 5G network equipment. Eight officials indicated actions to increase 5G regulations were extremely or very likely in Germany, Colombia, Australia, Czech Republic, Italy, France, and South Korea. Such action was considered unlikely by representatives of Japan, Colombia, and the EU. See also Declan Ganley, "Huawei/ZTE & 5G," *Rivada Networks*, November 12, 2019, <https://twitter.com/declanganley/status/1194291318488469504/photo/1>.

91. Related proposals on this front include, for example, "National Security Senators Introduce Bipartisan Legislation to Develop 5G Alternatives to Huawei," *Office of Senator Mark Warner*, January 14, 2020; Kiran Stacey, "US pushes to fund Western rivals to Huawei," *Financial Times*, October 7, 2019.

92. Daniel Kliman recommends that the United States launch a digital development fund. See Daniel Kliman, "Why the United States Needs a Digital Development Fund," *Center for a New American Security*, October 2019. On the EU's Digital4Development initiative, see Commission Staff Working Document: Digital4Development: mainstreaming digital technologies and services into EU Development Policy," EU Commission, Brussels, May 2, 2017.

93. "Net ODA," *Organisation for Economic Cooperation and Development*, 2019, <https://data.oecd.org/oda/net-oda.htm#indicator-chart>; "Foreign direct investment, net outflows (BoP, current US\$)," *International Monetary Fund*, Balance of Payments database, supplemented by data from the United Nations Conference on Trade and Development and official national sources, 2019, <https://data.worldbank.org/indicator/BM.KLT.DINV.CD.WD>; "2018 E-Government Development Index," UN E-Government Knowledgebase, 2018, <https://publicadministration.un.org/egovkb/en-us/data/compare-countries>; Bhaskar Chakravorti and Ravi Shankar Chaturvedi, "Digital Planet 2017," The Fletcher School at Tufts University, May 2017, [https://sites.tufts.edu/digitalplanet/files/2017/05/Digital\\_Planet\\_2017\\_FINAL.pdf](https://sites.tufts.edu/digitalplanet/files/2017/05/Digital_Planet_2017_FINAL.pdf); "Commitment to Development Index: Technology," *Center for Global Development*, September, 2018, [https://www.cgdev.org/commitment-development-index-2018#CDI\\_TEC](https://www.cgdev.org/commitment-development-index-2018#CDI_TEC).

94. Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative," *Council on Foreign Relations*, May 21, 2019, <https://www.cfr.org/backgrounders/chinas-massive-belt-and-road-initiative>.

95. Scholar Ben Buchanan introduces and elaborates on the distinction between signaling and shaping in his analysis of the geopolitics of cyber operations. See Ben Buchanan, *The Hacker and The State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge: Harvard University Press, 2020).

96. Hannas and Chang, "China's Access to Foreign AI Technology."

97. Elsa Kania, "China's Threat to American Government and Private Sector Research and Innovation Leadership," *Center for a New American Security*, July 2018, <https://www.cnas.org/publications/congressional-testimony/testimony-before-the-house-permanent-select-committee-on-intelligence>.

98. Ryan Fedasiuk, *Center for Security and Emerging Technology*, forthcoming research.

99. Noah Barkin, "Exclusive: Five Eyes intelligence alliance builds coalition to counter China," *Reuters*, October 12, 2018, <https://www.reuters.com/article/us-china-fiveeyes/exclusive-five-eyes-intelligence-alliance-builds-coalition-to-counter-china-idUSKCN1MM0GH>.

100. Ibid; James Stavridis, "The Western Allies Need More Eyes on the World." *Bloomberg*, May 3, 2019, <https://www.bloomberg.com/opinion/articles/2019-05-03/eyes-in-the-sky-the-west-needs-a-bigger-intelligence-network>.

101. Jim Bexfield and Ben Taylor, "Organization of Operations Research in the Five Eyes Countries," *Phalanx* 45, no. 3 (2012): 20-22.
102. Ryan Daws, "Britain successfully trials AI in battlefield scanning experiment," *AI News*, September 24, 2018, <https://www.artificialintelligence-news.com/2018/09/24/britain-trials-ai-battlefield-experiment/>.
103. Corey Pfluke, "A history of the Five Eyes Alliance: Possibility for reform and additions: A history of the Five Eyes Alliance: Possibility for reform and additions," *Comparative Strategy* 38, no. 4 (2019): 302-315.
104. OECD, "About the OECD," <https://usoecd.usmission.gov/our-relationship/about-the-oecd/what-is-the-oecd/> (Accessed on October 23, 2019).
105. OECD Legal Instruments, "Recommendation of the Council on Artificial Intelligence," OECD, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (Accessed on October 23, 2019).
106. Anne Carblanc, "AI at the OECD," *Organization for Economic Cooperation and Development*, February 14, 2019, <http://www.oecd.org/parliamentarians/meetings/gpn-meeting-february-2019/Ane-Carblanc-Artificial-Intelligence-14-Feb-2019.pdf>.
107. OECD Legal Instruments, "Recommendation of the Council on Artificial Intelligence," *Organization for Economic Cooperation and Development*, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (Accessed on October 23, 2019).
108. "Artificial Intelligence," *Organization for Economic Cooperation and Development*, <https://www.oecd.org/going-digital/ai/> (Accessed on January 2, 2019).
109. OECD Legal Instruments, "Recommendation of the Council on Artificial Intelligence," *Organization for Economic Cooperation and Development*, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (Accessed on October 23, 2019).
110. "OECD AI Policy Observatory," *Organization for Economic Cooperation and Development*, September 2019, <http://www.oecd.org/going-digital/ai/about-the-oecd-ai-policy-observatory.pdf>.
111. "Going Digital Toolkit," *Organization for Economic Cooperation and Development*, <https://goingdigital.oecd.org/en/> (Accessed on October 23, 2019); "OECD Digital Economy Outlook 2017," *Organization for Economic Cooperation and Development*, July 27, 2017, <https://www.oecd-ilibrary.org/docserver/9789264276284-en>.
112. Susan Mendonca, "The role of the OECD in shaping EU trade policy," *European Parliament Policy Department*, January 2016, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/570455/EXPO\\_BRI\(2016\)570455\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/570455/EXPO_BRI(2016)570455_EN.pdf).
113. "About ICDPPC," *The International Conference on Data Protection and Privacy Commissions*, October 3, 2008, <https://privacyconference2019.info/about/about-icdppc/> (Accessed on October 23, 2019).
114. Calli Schroeder, "When the world's DPAs get together: Resolutions of the ICDPPC," *International Association of Privacy Professionals*, November 28, 2017, <https://iapp.org/news/a/when-the-worlds-dpas-get-together-resolutions-of-the-icdppc/> (Accessed on October 23, 2019); 40TH International Conference of Data Protection and Privacy Commissioners "Resolution to Amend the ICDPPC Rules and Procedures," *The International Conference on Data Protection and Privacy Commissions*, October 23, 2018, 6.
115. "Enforcement Cooperation Resources," *The International Conference on Data Protection and Privacy Commissions*, <https://icdppc.org/enforcement-cooperation-repository/enforcement-cooperation-resources/> (Accessed on October 23, 2019).



116. 40th International Conference of Data Protection and Privacy Commissioners "Declaration on Ethics and Data Protection in Artificial Intelligence," *The International Conference on Data Protection and Privacy Commissions*, October 23, 2018.
117. 39th International Conference of Data Protection and Privacy Commissioners, "Resolution on Data Protection in Automated and Connected Vehicles," *The International Conference on Data Protection and Privacy Commissions*, September 25-29, 2017.
118. Christopher A. Ford, "Huawei and its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications," U.S. Department of State, September 11, 2019, <https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/> (Accessed on October 23, 2019); Christopher A. Ford, "Bureaucracy and Counterstrategy: Meeting the China Challenge," U.S. State Department. September 11, 2019, <https://www.state.gov/bureaucracy-and-counterstrategy-meeting-the-china-challenge/> (Accessed on October 23, 2019).
119. Ibid.
120. Ibid.
121. "Joint Statement of the 23rd Meeting of the World Semiconductor Council (WSC)," *World Semiconductor Council*, May 23, 2019.
122. "Issues/Activities," *World Semiconductor Council*, <https://www.semiconductorcouncil.org/issuesactivities/> (Accessed on October 23, 2019).
123. "WSC Public Documents and White Papers," *World Semiconductor Council*, <http://www.semiconductorcouncil.org/public-documents/public-documents-and-white-papers/> (Accessed on October 23, 2019).
124. "Purpose & Basic Principles," *World Semiconductor Council*, <http://www.semiconductorcouncil.org/about-wsc/purpose-basic-principles/> (Accessed on October 23, 2019).
125. "About SEMI," *SEMI*, <https://www.semi.org/en/about> (Accessed on October 23, 2019).
126. "Window On China Resources," *SEMI*, <https://www.semi.org/en/news-resources/window-on-china/presentations-resources> (Accessed on October 23, 2019); "Window on China Recent News," *SEMI*, <https://www.semi.org/en/news-resources/window-on-china> (Accessed on October 30, 2019).
127. Lung Chu, "The Rise of China IC Industry – Innovation and Investment Forum," July 11, 2017, <http://www1.semi.org/en/sites/semi.org/files/data17/docs/The%20Rise%20of%20China%20IC%20Industry.pdf>.
128. "Heterogeneous Integration Roadmap," *SEMI*, <http://www1.semi.org/en/heterogeneous-integration-roadmap> (Accessed on October 23, 2019).
129. "Collaborate," *SEMI*, <https://www.semi.org/en/collaborate> (Accessed on October 23, 2019).
130. "Our Mission," *World Economic Forum*, <https://www.weforum.org/about/world-economic-forum> (Accessed on October 23, 2019).
131. "Delivering Digital Infrastructure Advancing the Internet Economy," *World Economic Forum and Boston Consulting Group*, April 2014.
132. "Generation AI Establishing Global Standards for Children and AI," *World Economic Forum*, June 2019.
133. Our Vision," *International Telecommunication Union*, <https://www.itu.int/en/about/Pages/vision.aspx> (Accessed on October 23, 2019).

134. "FG-ML5G," *International Telecommunication Union*, <https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx> (Accessed on October 23, 2019).
135. "FG-AI4H," *International Telecommunication Union*, <https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx> (Accessed on October 23, 2019).
136. "AI for Good Global Summit 2017," *International Telecommunication Union*, <https://www.itu.int/en/ITU-T/AI/Pages/201706-default.aspx> (Accessed on October 23, 2019).
137. "About International Telecommunication Union (ITU)," *International Telecommunication Union*, <https://www.itu.int/en/about/Pages/default.aspx> (Accessed on January 3, 2020).
138. "All about Infrastructure Sharing 2018," *International Telecommunication Union*, July 2018.
139. "What Is the G20 Summit?" *Group of Twenty*, <https://g20.org/en/summit/about/> (Accessed on October 23, 2019).
140. Barbara C. Mathews, "When The G20 Met #AI," *The Medium*, July 1, 2019, <https://medium.com/swlh/when-the-g20-met-ai-d9e8b439ddf5>.
141. "G20 Osaka Leaders' Declaration," *Group of Twenty*, June 2019.
142. "About ADB," *Asian Development Bank*, <https://www.adb.org/>, (Accessed on October 23, 2019).
143. "Digital Agenda 2030: Special Capital Expenditure Requirements for 2019-2023," *Asian Development Bank*, October 2018.
144. "ADB Establishes High-Level Advisory Group for Digital Technology," *Asian Development Bank*, September 2, 2018, <https://www.adb.org/news/adb-establishes-high-level-advisory-group-digital-technology>.
145. "About Us," *International Organization for Standardization*, <https://www.iso.org/about-us.html> (Accessed on October 23, 2019).
146. Antoinette Price, "First International Standards committee for entire AI ecosystem," *International Electrotechnical Commission*, March 2018, <https://iecetech.org/Technical-Committees/2018-03/First-International-Standards-committee-for-entire-AI-ecosystem>.
147. Ibid.
148. "ISO/IEC JTC 1/SC 42 Artificial Intelligence," *International Organization for Standardization*, <https://www.iso.org/committee/6794475.html> (Accessed on October 23, 2019).
149. "What We Do," *World Bank*, <https://www.worldbank.org/en/what-we-do> (Accessed on October 23, 2019).
150. "Digital Development Partnership (DDP)," *World Bank*, <https://www.worldbank.org/en/programs/digital-development-partnership#1> (Accessed on October 23, 2019).
151. "Artificial Intelligence for Economic Development," *CEGA and World Bank*, March 1, 2018, <https://www.measuredev.org/>.
152. "The Launch of The Future Society-World Bank joint report," *The Future Society*, <https://thefuturesociety.org/events/launch-of-world-bank-report/> (accessed on October 29, 2019).
153. "What we do," *World Trade Organization*, [https://www.wto.org/english/thewto\\_e/whatis\\_e/what\\_we\\_do\\_e.htm](https://www.wto.org/english/thewto_e/whatis_e/what_we_do_e.htm) (Accessed on October 23, 2019).
154. "China says U.S. controls on semiconductor firm break WTO rules," *Reuters*, November 13, 2018, <https://www.reuters.com/article/usa-trade-china-semiconductors/china-says-us-controls-on->

semiconductor-firm-break-wto-rules-idUSL8N1XO3QS; "Comments Concerning Proposed Modification of Action Pursuant to Section 301: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation," SEMI, June 2019.

155. Peter John Williams, "Accession in Perspective," in *Accession to the WTO*, (Cambridge, UK: Cambridge University Press, 2008).

156. "About 3GPP," 3rd Generation Partnership Project, <https://www.3gpp.org/about-3gpp> (Accessed on October 23, 2019); "Partners," 3rd Generation Partnership Project, <https://www.3gpp.org/about-3gpp/partners> (Accessed on October 23, 2019).

157. "About 3GPP," 3rd Generation Partnership Project, <https://www.3gpp.org/about-3gpp> (Accessed on October 23, 2019).

158. "Evolution to an Artificial Intelligence-Enabled Network," *Alliance for Telecommunications Industry Solutions*, September 2018.

159. "The IMF at a Glance," *International Monetary Fund*, March 22, 2019, <https://www.imf.org/en/About/Factsheets/IMF-at-a-Glance>.

160. "Fintech and the IMF," *International Monetary Fund*, <https://www.imf.org/en/About/Key-Issues/Fintech> (Accessed on October 23, 2019).

161. "IMF Policy Paper Fintech: The Experience So Far," *International Monetary Fund*, June 28, 2019.

162. "The IMF at a Glance," *International Monetary Fund*, March 22, 2019, <https://www.imf.org/en/About/Factsheets/IMF-at-a-Glance>.

163. "2019 OSCE Annual Police Experts Meeting: Artificial Intelligence and Law Enforcement – An Ally or Adversary," *Organization for Security and Co-operation in Europe*, <https://www.osce.org/event/2019-annual-police-experts-meeting> (Accessed on October 23, 2019).

164. "Decision No. 5/19 Human Capital Development in the Digital Era," *Organization for Security and Co-operation in Europe*, December 7, 2018.

165. "Policing," *Organization for Security and Co-operation in Europe*, <https://www.osce.org/policing> (Accessed on January 3, 2020).

166. Bardi Veeraghanta, "Digitalisation key to ASEAN attracting China trade war exodus," *The Business Times*, October 23, 2019, <https://www.businesstimes.com.sg/asean-business/digitalisation-key-to-asean-attracting-china-trade-war-exodus> (Accessed on October 23, 2019); "About ASEAN," *Association of Southeast Asian Nations*, <https://asean.org/asean/about-asean/> (Accessed on October 23, 2019).

167. "Empowering Micro, Small and Medium Enterprise Towards a Digital ASEAN," *Association of Southeast Asian Nations*, June 26, 2019, <https://asean.org/empowering-micro-small-medium-enterprise-towards-digital-asean/?highlight=digital>.

168. "ASEAN Foundation selects 17 science and technology fellows," *Association of Southeast Asian Nations*, June 27, 2018, <https://asean.org/asean-foundation-selects-17-science-technology-fellows/?highlight=artificial%20intelligence>.

169. "D9-Charter," D9, November 22, 2018, <https://leadingdigitalgovs.org/comunicacion/publicaciones/d9-charter>.

170. "Canada welcomes leading digital nations into the Digital 9," *Treasury Board of Canada Secretariat*, November 22, 2018, <https://leadingdigitalgovs.org/politicas-y-gestion/israel-summit>; "Israel Summit," D9, November 20, 2018, <https://leadingdigitalgovs.org/politicas-y-gestion/israel-summit>.



171. "Data 360°," D9, June 24, 2019, <https://leadingdigitalgovs.org/comunicacion/noticias/data-360deg>.
172. "About Us," *The Wassenaar Arrangement*, <https://www.wassenaar.org/about-us/> (Accessed on January 3, 2020).
173. "List of Dual-Use Goods and Technologies and Munitions List, Category 3-Electronics," *The Wassenaar Arrangement*, May 12, 2019, 54.
174. Tom Cross, "New Changes to Wassenaar Arrangement Export Controls Will Benefit Cybersecurity," *Forbes*, January 16, 2018, <https://www.forbes.com/sites/forbestechcouncil/2018/01/16/new-changes-to-wassenaar-arrangement-export-controls-will-benefit-cybersecurity/#68516cf85ed6>.
175. Ibid.







CSET.GEORGETOWN.EDU | CSET@GEORGETOWN.EDU