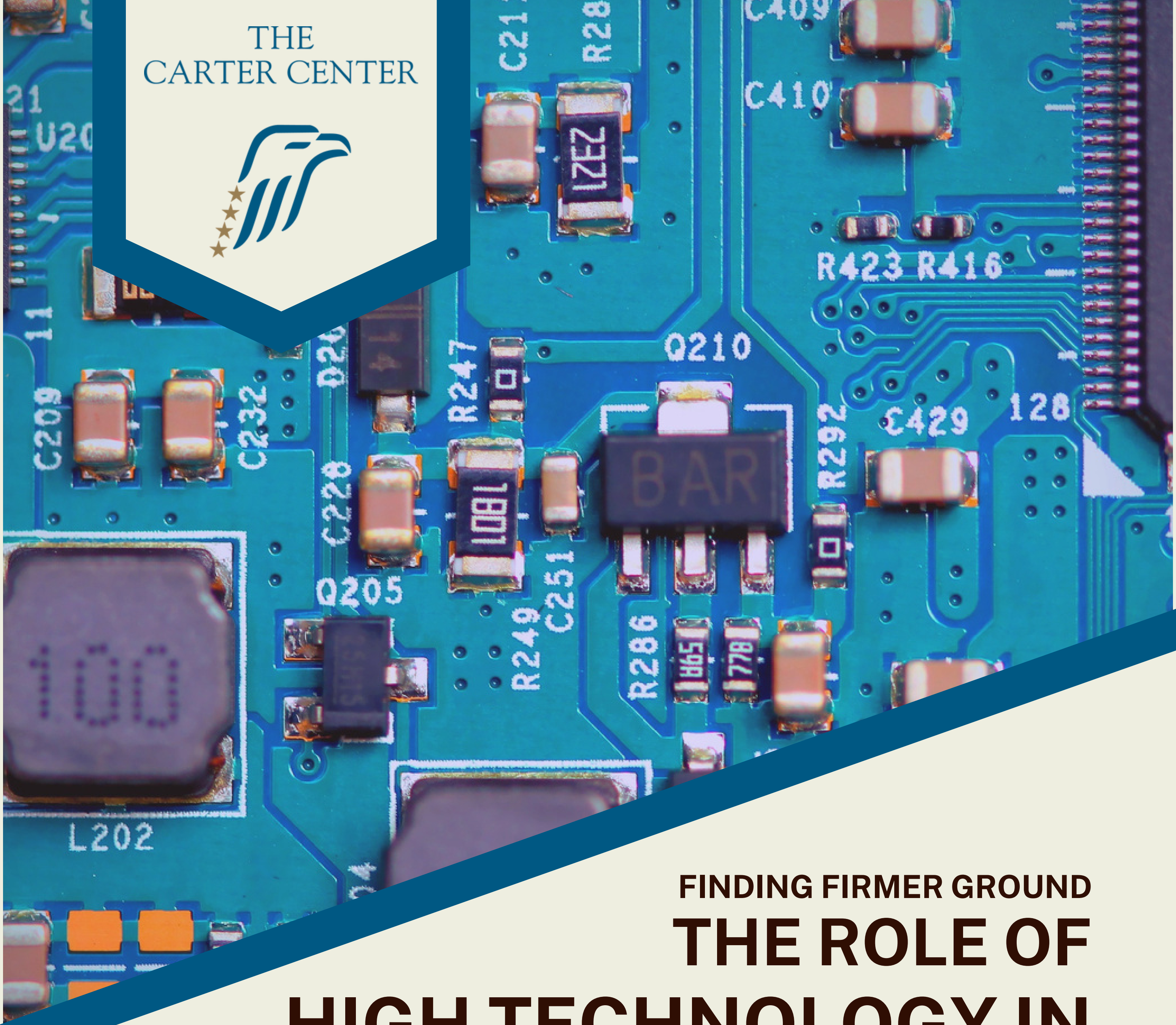
THE CARTER CENTER



FINDING FIRMER GROUND

THE ROLE OF HIGH TECHNOLOGY IN U.S.-CHINA RELATIONS

Sara Hsu

Ja-Ian Chong

Rorry Daniels

Shirley Martey Hargis

John Lee

Understanding the influence of high technology on U.S.-China relations, competition, and the prospects for cooperation.

Edited by Yawei Liu & Michael Cerny

Foreword by Victor C. Shih

Table of Contents

THE
CARTER CENTER

Peace. Fighting Disease. Building Hope.

The Carter Center is an independent, nonpartisan, nongovernmental organization founded in 1982 by former U.S. President Jimmy Carter and his wife, Rosalynn. The Carter Center seeks to prevent and resolve conflicts, enhance freedom and democracy, and improve health.

Authors

Sara Hsu *is a clinical associate professor of supply chain management at the University of Tennessee at Knoxville. Prior to that, she was an associate professor of economics at the State University of New York at New Paltz. Dr. Hsu specializes in Chinese supply chains, fintech, economic development, and shadow banking. Hsu earned her Doctor of Philosophy degree from the University of Utah, her Master of Business Administration from the University of Tennessee at Knoxville, and her Bachelor of Art's Degree from Wellesley College.*

Ja-Ian Chong *is associate professor of political science at the National University of Singapore and a non-resident scholar with Carnegie China. He received his Doctor of Philosophy degree from Princeton University in 2008 and previously taught at the Hong Kong University of Science and Technology. His research covers the intersection of international and domestic politics, with a focus on the externalities of major power competition, nationalism, regional order, security, contentious politics, and state formation.*

Rorry Daniels *is the managing director of Asia Society Policy Institute (ASPI), where she leads and oversees strategy and operations for ASPI's projects on security, climate change, and trade throughout Asia. She is also a senior fellow with ASPI's Center for China Analysis. She was previously with the National Committee on American Foreign Policy, where she managed the organization's Track II and research portfolio on Asia security issues, with a particular focus on cross-Taiwan Strait relations, U.S.-China relations, and the North Korean nuclear program.*

Shirley Martey Hargis *is a nonresident fellow in the Atlantic Council's Global China Hub and Digital Forensic Research Lab. She is also a consultant on the China and international security for CRDF Global's Data and Technology program. She has over a decade of experience in the domestic politics and foreign affairs of China and Taiwan. Hargis focuses on China's resurgence and cross-Strait tensions, including China's affairs in Africa, Russia, and Latin America. Her domestic and foreign policy expertise span defense and security, economics, and technology in consulting, intelligence, and policy research.*

John Lee *is the director of East West Futures Consulting, researching China's impacts on a world increasingly linked through digital technologies. Based in Europe and having previously worked for the Australian government, his analysis is informed by a sophisticated understanding of the political, business, and security environments in the EU, Australia, and east-southeast Asia.*

I. Foreword

By Victor C. Shih, Ho Miu Lam Chair Associate Professor in China and Pacific Relations at the School of. Global Policy and Strategy at the University of California, San Diego specializing in China

China's accession to the World Trade Organization (WTO) marked the high-water point of bilateral relations between the U.S. and China. China was still technologically far behind the U.S. and other Organization for Economic Co-operation and Development (OECD) countries as U.S. companies looked for a large pool of cheap and adequately skilled labor. With the lowering of tariffs on Chinese-made goods after China's WTO accession, the two countries enjoyed a decade and a half of enormous mutual gains that lowered the cost of the digital revolution in the U.S. and lifted hundreds of millions out of poverty in China. The Chinese government also took advantage of foreign investment to absorb technologies from foreign companies and to use greater fiscal resources to build up its military and bolster industrial policy. Today, bilateral trade amounts to over $1 trillion a year, which continues to provide ample mutual benefit to firms and individuals across the two countries.

Yet, the narrowing asymmetry of power and technology have bred deeper mistrust and even hostility between the two countries. Since 2012, Chinese General Secretary Xi Jinping's attempts to highlight China as a premier power in the world has encouraged hawks in the U.S. government to move China to the "center stage" of U.S. foreign policy with an increasing focus on China as the main competitor and strategic threat to the U.S. This report starts from a place that many from both sides can heartily agree — that the downward spiral in bilateral relations over the past six years must be managed more effectively in order to prevent worse dynamics from taking hold.

In addition, the authors, all seasoned China watchers and experts in technology policy, identify several core logics instilling distrust and overall insecurity among policymakers on both sides. They then propose potential policies to mitigate these sources of mistrust and insecurity. Fundamentally, the points raised in this report narrow down to one powerful source of insecurity, the anarchic nature of the global order, along with one strong motivation for cooperation: the profit potential of the technology industry. Taken together, these provide some hope for realistic cooperation and conflict management, which the report sets forth.

First, for years, China has taken advantage of the anarchic nature of the global order to steal billions of dollars in intellectual property (IP) from more advanced countries.

Since Chinese companies stealing technology were beyond U.S. jurisdiction, there was little that U.S.-based claimants could do to enforce American IP law on companies thousands of miles away and in other jurisdictions. The WTO provided a cumbersome mechanism for companies to lodge IP-related grievances, but it moved slowly and ultimately had no means of enforcing rulings on convicted parties (or at least no enforcement that the guilty party could not circumvent quickly). Again, this was not a problem when the technological disparity between the U.S. and China was vast. By 2010, however, Chinese technology companies like Huawei were taking market share from leading U.S. firms like Motorola and Cisco. The prospect of inadvertent or deliberate technology transfer has become a major worry among U.S. policymakers, especially in the integrated circuits (IC) sector. As the report outlines, the U.S. has rolled out a series of sanctions against the Chinese IC industry to prevent further technological leakage, going so far as to bar U.S. citizens from working for Chinese IC firms. These measures were rolled out because transnational law enforcement remains limited, so the U.S. felt compelled to maximize the reach of domestic jurisdictions to sanction individuals and companies that are domiciled in the U.S. or conduct extensive business with U.S. entities.

Even in the cybersecurity realm, the inherently anarchic nature of the global order constitutes a root problem. If the U.S. federal government wants to hack into the computer of a domestic company, it needs to obtain a court order to do so, which leaves a paper trail and potential liability. A U.S. court also can stop the government from hacking domestically, which law enforcement authorities, in theory, will enforce. However, beyond the national border, nothing save for occasional congressional oversight stops a U.S. government agency from hacking into a foreign company's computer. Likewise, nothing short of a threat of retaliation stops Chinese agencies from hacking into U.S. computers. If governments around the world see retaliation as the only effective deterrent to hacking, they will engage in a constant series or hacks and counter-hacks, resulting in untold economic losses to the major powers and any countries without adequate know-how to defend themselves.

On the other hand, the authors of this report suggest that both sides have some incentive to engage in dialogue and regulatory coordination. Why would these two competing powers do that? We must recall that bilateral trade and investment has generated hundreds of billions of dollars in profits for companies on both sides. Even in the IC sector, which now is a $500 billion-a-year industry, the potential for mutual gains is enormous.

To be sure, in some areas, the relationship between the two countries is akin to a prisoner’s dilemma game where cooperation by one side leads to a “sucker’s” payoff and absolute gain by the other side. For example, agencies on both sides will continue to hack into the other’s government. The side that doesn’t will lose out.

Still, in other areas, coordination between the two countries will lead to gains for both sides and the lack of cooperation even by one side will lead to losses for both. In the area of renewable energy, for example, both sides have strong incentives to coordinate. Both sides will benefit from faster adoption of electric vehicles, and U.S. carmakers can benefit from the lower costs of Chinese batteries. Chinese battery makers can make money off U.S. buyers of Chinese batteries. For the U.S., increasing dependence on Chinese batteries is not such a problem since it still has plenty of oil if China were to impose a battery embargo on the U.S.

The challenge for both sides, as highlighted by the report, is to harmonize domestic or global regulations to structure incentives for coordination by both sides. Already, the U.S. has started to harmonize its state capacity in the high-tech realm so that it can match the robust technology policies of China. This should not be seen by China as an unmitigated negative development. It actually helps the U.S. government obtain better information from sectoral players about optimal policy approaches and craft intermediate policy solutions. The report makes the very sensible suggestion of forming a global regulatory body for Internet of Things (IoT) technology so that privacy standards can be coordinated and even enforced. This is an excellent suggestion. I would add that perhaps blockchain technology can be brought to bear to help with enforcement. For example, the vendor of a new IoT device must submit a blueprint of its product, which complies with a certain set of privacy requirements. The vendor must further deposit a substantial sum of money in an escrow account. If members of the governing body find a deviation in the vendor’s product from its original blueprint that jeopardizes privacy, a blockchain contract is immediately executed to take the vendor’s deposit, thus creating a financial loss for the offender. In general, the crafting of fair and transparent mechanisms with a bite will make transnational coordination in digital regulation more tractable.

In sum, competition between two sovereign nations is always tricky due to countries’ inability to enforce laws on one another. However, commercial incentives, transparency, and technologies that ensure transparency provide some grounds for cooperation and conflict management in the future.

II. Executive Summary

In the past decade, China and the U.S. have found themselves increasingly in dispute over issues like the South China Sea and Taiwan, and these disagreements have only intensified in recent years. Conflict between the U.S. and China is escalating, starting with the trade war under the Trump administration on economic and technological fronts and later expanding into the realm of human rights, governance, and semiconductor competition under the Biden administration. As tensions have risen and attempts to defuse conflict have dwindled, the chance that the two countries become entangled in greater strife has increased.

One of the central sources of friction relates to the emergence and use of new technologies, which have opened not only new realms of opportunity but also potential for exploitation. Today, new technologies and their applications are complex, underregulated, and thought to be farther-reaching than previous technology regimes. The fact that both nations are attempting to compete fiercely across the range of new technologies has situated the U.S. and China as strategic competitors.

Both nations have competitive advantages that set them apart from one another. On one hand, the U.S. has a well-funded private sector that innovates mainly for the consumer. On the other hand, China has a state-funded apparatus for both state- and privately owned enterprises that innovates based on state policy objectives. It is this competitive advantage, China's state-driven approach, that principally concerns American values surrounding personal privacy and competition. Conversely, some Chinese resent the United States' protective attitude toward technology, which, in their view, seeks to prevent other nations from reverse engineering or simply using proprietary technology.

Due to the complexity of technology, intellectual property theft, competing state approaches, and clashing values over privacy have created major challenges to American and Chinese companies operating cross-nationally. Even where there is a clear legal structure governing technology use, concerns remain over legal enforcement and the ultimate control of such technology. In this report, we review major new technologies, discuss the issues at stake between the U.S. and China, and describe ways that both countries can find firmer ground to coexist peacefully. We specifically examine artificial intelligence, the Internet of Things, big data and privacy, semiconductors, and cyberattacks, and conclude with suggestions for constructive dialogue.

Artificial Intelligence. Artificial intelligence can simulate human thought and reactions using large data sets and has both civilian and military applications. AI-based applications can be used for business purposes, to provide customers with the highest service levels. The technology has been used, for example, to improve credit scoring for small businesses and to customize product marketing to individual preferences. At the same time, AI can also be applied to enhance the effectiveness of cyberattacks or to monitor people.

One of the biggest concerns surrounding AI relates to different views about human rights and legal enforcement in China and the U.S. Culturally, Americans have often emphasized the protection of individual rights, while the Chinese tend to emphasize the rights and security of society as a whole. In addition, the relationship between AI and the legal system differs in both countries. While both the U.S. and China use AI facial recognition technology to monitor citizens, for example, there are key differences as to how citizens are identified as national security threats and in provision of due process.
In addition to these differences, the U.S. has criticized China for competing unfairly by involving the state in innovation.[1] Notably, the U.S. government is increasingly involved in setting innovation and technology competition policy. Both the U.S. and China have AI strategies created by their respective governments, but the Chinese strategy is more comprehensive. The Ministry of Science and Technology and the Ministry of Industry and Information Technology develop research in this area and bring new technologies to industry. In addition, China has integrated AI development into its policy plans since the controversial Made in China 2025 plan was released in 2015, furthering China’s role as “strategic competitor” to the U.S.

Due to fundamental differences in views of human rights and the role of the state in innovation, the U.S. and China will continue to struggle to find common ground on this technology. However, the ability to avoid escalation of future conflicts is essential to building trust on this issue. The establishment of conditions that help to increase transparency and can provide a means for de-escalation in the event of conflict will improve the chances of maintaining a peaceful relationship.

Internet of Things. The Internet of Things or “IoT” refers to the interconnected devices that people use daily, including the networks, data, and computational processes supporting technological devices. For example, the internet is no longer people to people, but “things” to “things” linked together through internet connectivity and controlled via cyberspace. Oftentimes, the interconnectivity of devices is not mediated by humans, resulting in a significant increase of interconnected cyber-physical systems.

IoT can be used for both civilian and military purposes and has been incorporated into smart cities and smart schools as well as into weapons systems and aircraft. These objects can collect and transmit large amounts of data, but increased connectivity comes with greater risk of cyberattacks. Coupled with other new technologies, including 5G and artificial intelligence, IoT presents new security challenges. Hackers have been able to gain access to vulnerable networks by gaining access to IoT objects, including surveillance cameras.

China has streamlined policies to integrate IoT into everyday life across a variety of industries, including the urban construction, medicine, and automotive industries. Policies made at the central level have promoted IoT as a strategic emerging industry. The country also has policies to protect privacy rights against IoT devices.
The U.S. has focused on preventing sale of critical technologies to China to maintain its technological superiority. The Trump administration went further to ban U.S. companies from engaging in commerce with Chinese companies that are considered a national security threat. President Biden extended this entity list to include firms and military research institutes, such as SenseTime Group Limited, Leon Technology Company Limited, and Yitu Limited.[2]

To find firmer ground, both the U.S. and China should ensure that the IoT must be sufficiently secured. Standardization can help to increase the security of IoT devices and ensure global market participation by increasing compatibility between systems.

Big Data and Privacy. Big data is comprised of large data sets that may include a variety of data types. The data can be used to reveal complex patterns of individual, firm, or system behavior. The main issue with big data is that it creates new vulnerabilities for security and privacy.

Both China and the U.S. are concerned about data privacy, in different ways. The U.S. is primarily concerned with protecting data that could expose individual financial and personal information. China is primarily worried about the collection of data by commercial entities and the potential for foreign espionage. Common concerns about data privacy can provide the two countries with a starting point for cooperation. This is especially an issue in the U.S., where there are no all-encompassing data privacy laws like China’s Personal Information Protection Law and Data Security Law.

Improvements in data protection and bolstered privacy standards in the U.S. are therefore critically important. Without a comprehensive data privacy law, the U.S. will struggle to launch a productive conversation with China on this topic.

The U.S. should remedy this gap and engage in an ongoing dialogue with China on cybersecurity issues. As this report explores, high-level negotiation has proved successful in the past. Collaboration between the U.S. and China, as well as other nations, can help reduce the risk of data exposure.

As in the case of artificial intelligence, the U.S. and China hold different views on who should have access to data. The Chinese state controls data generated within the state, while American individuals do not wish to grant the state access to their personal data. Such ideological differences must be taken into consideration in conversations between the two nations.

Semiconductors. Semiconductors are essential for most modern electronics and carry out a range of functions, including computational processing. The semiconductor industry is characterized by specialized division of labor across countries, with many steps dominated by just a few major firms. This creates nearly insurmountable challenges for individual countries to onshore complete semiconductor supply chains.
In recent years, the U.S. has imposed export controls on Huawei, SMIC, and other Chinese firms that require foreign technology, thereby slowing development of China's semiconductor industry. The U.S. is working to bring semiconductor production onshore, but despite the strengths of the American semiconductor industry, significant foreign dependency in certain areas will remain for many years to come.

China's semiconductor industry has made significant progress over the past two decades but generally remains well behind global industry leaders in most segments of the semiconductor supply chain. Despite top-level policy attention and significant state support for the industry, China remains heavily dependent on foreign equipment and overseas inputs.

Neither China nor the U.S. is likely to achieve success in capturing a significantly larger share of the global semiconductor supply chain for their companies over the short term. While the foundational nature of semiconductors as a technology means that prospects for cooperation are limited, both nations should try to limit antagonistic actions, such as expansion of export controls or punitive retaliatory measures.

The way forward. Technology comprises innovations that arise and operate within an existing political and social context. Different ideological approaches to technology have given rise to mistrust between the U.S. and China. A mutual dialogue cannot occur without understanding and accepting these fundamental differences, such as with respect to private and state-led innovation.

Differences in operating procedures for dialogue and diplomacy have given rise to negotiation fatigue. Stronger engagement requires mutual understanding of risk perceptions and the desire to work toward common rules and standards for technology use. Building trust between the two nations will provide a better understanding of the other side's intentions.

We suggest a roadmap to more productive bilateral dialogue. This includes the following recommendations:

1. ***Each side must keep expectations realistic.*** Managing expectations for future compromise on the different issues is essential to measuring success. Neither side should come into dialogue anticipating that the other side will make sweeping changes in its approach to technology competition or the role of technology in society. Instead, the focus should be on better understanding the evolving state position on underlying and emerging issues. This can help to shape bilateral consensus on basic principles.

2. ***Dialogues must get the right people together.*** Use of various new technologies cuts across multiple government agencies in both countries, and it is important to identify the correct personnel to communicate with, both in government and in the private sector where necessary.

3. ***The two sides should set a workable agenda.*** Neither side is likely to want to share specific intellectual property but rather may wish to focus on the extreme ends of the spectrum — the broadest and the narrowest issues. As grounds for engaging in productive dialogue, each side must clearly understand the other side's interpretation of rules of fair use of cyber tools.

4. ***The dialogue must take place on a regular schedule.*** This can prompt regular internal policy reviews on either side in preparation for meetings that strive to keep pace with rapidly evolving innovation.

5. ***The dialogue framework should balance the interplay between bilateral discussions and international institutions and agreements.*** Not only should the U.S. and China consider bilateral agreement and agendas, but the participants also should consider the expansion of such principles and discussions to larger multilateral formats.
New technology does not have to derail diplomacy and should be used to strengthen rather than weaken political relations between countries.

Notes:

[1] See the USTR's Section 301 Findings on China's technology practices,https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

[2] Barker et al. 2022, Biden Administration Issues New Sanctions and Trade Restrictions on Chinese Technology Entities and Adds 34 Chinese Entities to the Entity List, Arnold and Porter Advisory, January 7. https://www.arnoldporter.com/en/perspectives/advisories/2022/01/biden-issues-new-sanctions-on-chinese-technology

III. Introduction

As competition between the U.S. and China escalates, there are questions about how each country will use technology to further their economic and political interests. There are several issues that present potential threats to a peaceable relationship between the two nations. Although the U.S. is considered a global leader in the field of artificial intelligence and other areas of technological development, China is rapidly catching up and concerns abound that such technology will be used to accelerate cyberattacks.
At the core of the technology conflict are differences in how each country perceives individual rights and the role of the state. The U.S. places significant weight on values relating to individual privacy and freedom, while China views stability and state security as paramount. Maintaining peace while advancing technological innovation requires recognition and acceptance of these different values.

Newly developed technologies themselves present complex challenges to state values. Artificial intelligence requires the construction of ethical guidelines that were previously unnecessary. Access to semiconductors and the U.S.-China semiconductor competition challenge the nature of and rules of globalization. Moreover, technologies such as the Internet of Things and big data greatly widen the scope of technology's applications and create new vulnerabilities that can be exploited by third parties. These technologies are becoming increasingly widespread across industries. These include both civilian and military sectors, such as the health care, pharmaceutical, and transport industries, as well as the defense industry. In China, the state has explicitly encouraged the use of such technologies across sectors, while competition among firms in the U.S. has rendered the adoption of new technologies a necessary tool for firm survival.

In the following sections, we look at key new technologies and the issues they present for the U.S.-China relationship. We elaborate on existing and potential issues regarding new technologies. In each section, we examine how these individual technologies are embedded in the broader framework of U.S.-China competition, describe the U.S.' and China's existing policies in each technology area, and then describe overarching practices that could help reduce the potential for conflict with regards to their development or application . We conclude with a section about how dialogue can be enhanced to facilitate cooperation.

IV. Artificial Intelligence

The technology and its uses. Artificial intelligence (AI) combines with big data and the speed of cloud computing to simulate human thought and reactions. This process reduces the costs of doing business and can improve customer service and risk management. AI helps firms analyze patterns that may not be perceptible to humans to uncover business risks and process transactions.

However, artificial intelligence can be used for both civilian and military purposes. For example, AI systems can be designed to identify and exploit vulnerabilities in other systems. AI can also be used to attack systems, such as by using human-like behavior to crowd out legitimate users, identifying ideal targets in large data sets, and creating vulnerabilities in consumer machine learning models to distort results.

Overall, the U.S. possesses high levels of domestic and international AI talent and well-developed AI innovation and hardware systems. China has many AI patents and high venture capital investments, but fewer AI companies and lower levels of AI talent than the U.S. A major reason for this difference is that many Chinese AI researchers move to the U.S. to work for cutting-edge firms and institutions. While both countries are leaders in the number of AI companies, China is unique in developing specialized zones called New Generation AI Innovation Development Experimental Zones, where AI demonstrations and policy tests are carried out.

In addition, many AI-targeted microchips are developed by American companies, on which China is partially dependent. The U.S. dominates production of graphics processing units produced by American firms like Nvidia, Google's Tensor Processing Unit (TPU), and field programmable gate arrays (FPGAs) from companies like Intel and Xilinx.

U.S. companies also have an innovation edge in AI-enabled analytical tools. For example, the U.S. leads the world in claiming the top deep learning frameworks, TensorFlow developed by Google, and PyTorch, developed by Facebook.[1] The U.S. is also a leader in natural language processing, with over double the number of firms as China and triple the number of employees.[2] Moreover, the U.S. is a global leader in computer vision and autonomous driving.

Seeking to catch up to the U.S., China has used its large population and market to its advantage in recent years. China has made strides in obtaining data for AI training purposes because it has been able to take advantage of customer data and customer biometrics. Before the Personal Information Protection Law came into effect in October 2021, privacy laws were more lenient in China, which provided Chinese firms and government entities with rich databases on which to train artificial intelligence models. China also leads in speech recognition.

In addition, China has tasked selected private sector AI "champions" with specific innovations, such as Alibaba for smart cities and Baidu for autonomous vehicles. This status comes with enhanced access to state finance and preferential treatment in contract procurement.[3] Alibaba implemented the City Brain project across China to increase the speed and transparency of administrative processes and improve service delivery, such as in Hangzhou's Xiaoshan International Airport, where Alibaba technology was used to better manage airport schedules and maintenance.[4] Notably, some of the AI champions, including iFlyTek, SenseTime, and Huawei, have been banned in the U.S. on national security grounds and are not permitted to acquire hardware, software, and technology from American companies.

Some artificial intelligence software relies on visual recognition, and China's prowess in this area is undeniable. In 2016 and 2017, for example, Chinese scientists won first place at the Large Scale Visual Recognition Challenge for computer vision systems. Causing international outcry, China has deployed its advanced technology in this area to identify and trace individuals in China's Xinjiang Uyghur Autonomous Region (XUAR) who the state views as potential terrorists, often using race-based attributes. By using SenseTime's technology to compare faces stored in a database of known terrorist suspects with real-time surveillance footage, China's security apparatus is now able to identify and locate these suspects. Megvii's "Sharp Eyes" project accomplishes the same task across multiple provinces, including and beyond Xinjiang. Its cameras collaborate with the Integrated Platform for Joint Operations so that police officers can carry out facial identification at a wider scale.

This reflects a difference in ethical norms for technology use between the U.S. and China, as the Chinese government views the broad use of surveillance and facial recognition as tools for maintaining stability and security, whereas U.S. firms have restricted its use among the public to some extent on the basis of human rights and individual privacy. Sullivan (2021) argues that AI's surveillance capacity represents "the most significant single obstacle to cooperation on AI norms, rules, and procedures between our nations."[5] It should be noted, however, that U.S. agencies are using facial recognition in criminal investigations where criminal activity has been committed, and are planning to increase use of such software[6], even if facial recognition for the purposes of rating citizens and identifying suspicious behavior of noncriminals is not used as it is in China.

The GAO report on facial recognition states that 15 of the 42 federal agencies surveyed on the use of facial recognition software use nonfederal sources, with only one of these agencies keeping records of what nonfederal software is being used. Six of the agencies reported using the technology to identify suspects engaged in civil unrest, riots, or protests. By contrast, companies such as Facebook have eschewed the use of facial recognition due to concerns raised by privacy experts.

Natural language processing has allowed the Chinese government to identify individuals for national defense purposes. The company iFlytek uses natural language processing to assist the Ministry of Public Security in creating a national speech-pattern and voice database.[6] The National Security Agency in the U.S. also uses natural language processing to convert communications to text. In addition, the U.S. Defense Department’s Defense Advanced Research Projects Agency (DARPA) uses the Deep Exploration and Filtering of Text program to extract and act upon information across unstructured text data for the purposes of defense.[7] Executive Order 12333 on United States Intelligence Activities calls upon departments and agencies to provide “the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats.”[8] This order has permitted the U.S. government to monitor citizens without the use of a warrant, and it is unclear to what extent electronic surveillance is used.

Although both China and the U.S. are using AI to monitor citizens, albeit to varying extents, the underlying difference in attitudes toward human rights provides a basis for conflict between the two nations. What is at issue is less the use of technology to identify criminals than differences in what is outlawed. China has no protections in practice for freedom of speech or assembly and therefore classifies a wide range of government critics as national security threats. These include individuals who speak out against the state, such as lawyers, feminists, religious practitioners, and in many cases those belonging to ethnic minority groups. The U.S. also targets individuals who are considered national security threats under a narrower definition while generally upholding due process. The difference in attitudes toward human freedoms such as freedom of speech and religion, protection against unreasonable search and seizure, and due process has resulted in fear that the Chinese government will apply its internal standards of privacy to foreign users of its equipment and software. This fear is at the root of the conflict over AI monitoring and surveillance.

Compounding this fear is the fact that China has implemented AI in a more integrated fashion between its civil and military spheres, as opposed to the U.S., which faces a divided audience in AI implementation between the Pentagon and Silicon Valley.[9] As a result, Chinese tech firms have built in back doors or security vulnerabilities, possibly for the purposes of providing information about domestic Chinese users to the Chinese intelligence community. For example, a Chinese camera vendor, Xiongmai, was found to have created software containing an undocumented back door that could access millions of cameras. While some of the code may be prepared for China's domestic market, it is challenging to maintain separate software installations for devices sent to other destinations abroad. In other words, technology shipped from China may still contain this vulnerability[10], which can present problems for other states' national security.

There is also anxiety in the U.S. that China will use AI to counter traditional American defense-related espionage. The U.S. National Security Commission on Artificial Intelligence released its final report in March 2021,[11] which stated that China is a strategic competitor to the United States in AI. It further indicated that the U.S. is worried that China will use AI to identify and expose American sources and methods.

In addition, the U.S. views China's development of AI as a threat due to China's cyberattack targets. For example, China's hack of Microsoft Exchange is believed to be part of an unknown long-term artificial intelligence project.[12] The hack of email data was carried out by Hafnium, a In addition, the U.S. views China's development of AI as a threat due to China's cyberattack targets. For example, China's hack of Microsoft Exchange is believed to be part of an unknown long-term artificial intelligence project.[13] The hack of email data was carried out by Hafnium, a cyber-espionage group with alleged ties to the Chinese government. Cyberattacks can be made more rapidly, with better precision, and in greater secrecy with the use of AI. Cyberattacks have been used in recent years to steal trade and government secrets. There is a concern that use of AI-fused data for blackmail, deepfakes, or swarms are possible in the future. China has also allegedly used deepfakes to influence Taiwanese elections.[14]

China's fear of U.S. cyberattacks has likewise grown. Chinese media reports have stated that the U.S. is the largest source of cyberattacks in the country, attacking aerospace, scientific research institutions, large internet companies, and government agencies.[15] At the same time, there appears to be less fear in China that the U.S. will harness AI to augment cyberattack capabilities.

Finally, the U.S. believes that China can use AI to offset U.S. military superiority by implementing a type of "intelligentized war" that uses alternative logistics, procurement, training, and warfare algorithms.

In this scenario, battle networks will connect systems, and armed drones with autonomous functions will be employed. AI can also help to identify and hit valuable targets more rapidly. Notably, China has expressed the wish to ban usage, though not development, of autonomous lethal weapons.[16]

The Department of Defense's 2020 annual report to Congress on the Chinese military stated that China views new technologies as the means to engage in intelligentized warfare. This will speed up decision-making capabilities and improve intelligence and surveillance technologies. The People's Liberation Army even reorganized its research and education institutes to integrate new technologies with the development of new operational concepts in 2017.

The U.S. military also uses AI and possesses autonomous weapons. The U.S. has made use of the technology under Project Maven, which was tasked with identifying insurgent targets in Iraq and Syria. AI research is being conducted in the areas of intelligence collection and analysis, logistics, cyber operations, information operations, command and control, and semiautonomous and autonomous vehicles.[17] However, it is critical to note that the U.S. has a transparent policy on AI decision-making in offensive capabilities; it has published guidance on Autonomy in Weapon Systems, which requires "appropriate levels of human judgment over the use of force."[18]

As in the case of AI-based surveillance and data usage, U.S. anxiety over China's "intelligentized war" concept is based on China's record of behavior on other international norms and values. For example, Morgan et al. (2020) claim that China has not complied with biological and chemical weapons treaties, nor with its World Trade Organization obligations, leading to concerns over China's commitment to binding agreements.[19] In addition, China has proposed a ban on lethal autonomous weapon systems that defines such systems quite narrowly, and which is not supported by the US. This has led some observers to call into question China's true commitment to banning such weapons, especially as U.S. standards are currently stricter than those in China's proposed ban.

Still, the U.S. itself ignores international agreements when they fail to serve its interests. This has been a feature of American participation in the international arena since before its independence from Great Britain. More recently, the U.S. has withdrawn from the Paris Climate Accords and has violated WTO tenets under the Trump trade war. Although the Biden administration has sought to reinvest in international institutions and agreements, there are no guarantees that future administrations will maintain compliance and few punishments the international system can impose on its largest power for violating the rules.

Current policies. Both the U.S. and China have implemented policies to promote and safeguard new technologies. AI has received ample consideration by both governments. The Biden administration released a blueprint for a “bill of rights” in October 2022 to guide the design and implementation of technologies such as artificial intelligence. The objective was to ensure safe systems, protect individual privacy, and prevent algorithmic discrimination.[20]

Prior to that, on Feb. 11, 2019, President Trump signed Executive Order 13859, establishing the American Artificial Intelligence Initiative coordinated by the National Science and Technology Council Select Committee on Artificial Intelligence. This program coordinates AI activities across all federal departments and streamlines objectives related to improving access to federal data, models, and computing resources, lowering barriers to AI technology implementation, reducing vulnerability to attacks, training American AI researchers, and implementing a plan to safeguard U.S. economic and national security interests. The American AI Initiative sought to create a blueprint for setting up the National AI Research Resource. On March 19, 2019, the government released AI.gov, which provides the public with information on federal government activities in AI. The National AI Initiative Act of 2020 was released to coordinate federal government efforts to accelerate AI research and application.[21]

The U.S. National Artificial Intelligence Research and Development Strategic Plan, updated June 2019, aims to meet eight priorities in support of the AI Initiative: to make long-term investments in AI research, to develop methods for human-AI collaboration, to address ethical and legal aspects of AI, to ensure safety and security of AI systems, to develop shared data sets for AI training, to create benchmarks in AI, to understand AI R&D workforce needs, and to increase public-private partnerships for development of AI.[22] The Biden administration has set up this National Artificial Intelligence Research Resource Task Force to understand how to promote innovation.

The Department of Defense has published a classified AI strategy and carries out related tasks, such as setting up a Joint Artificial Intelligence Center to implement artificial intelligence technologies, publishing a roadmap for AI development, and creating a National Security Commission on Artificial Intelligence to assess military-related AI technologies and make recommendations for further implementation.[23] The report recommends that the U.S. achieve military AI readiness by 2025 through Pentagon leadership reforms and augmentation of the Department of Defense’s AI R&D portfolio.[24]

In China, the government plays a particularly important role in AI research and development. Both the Ministry of Science and Technology and the Ministry of Industry and Information Technology coordinate and develop research in this area. In addition, the Ministry of Industry and Information Technology plays an important role in bringing new AI technologies to industry. The NDRC's Department of High-Tech Industry also plays a key role in promoting technological advancement.

Like Biden's AI "bill of rights," China has released several regulations aimed to protect society. These include rules for online algorithms, certification of "trustworthy AI systems," and establishment of AI principles.[25]

China has a number of plans and policies that have integrated AI into state goals. The Made in China 2025 plan was released in May 2015 and aims to develop intelligent products and production. AI was also highlighted in the 13th Five-Year Plan, the Robot Industry Development Plan, the 13th Five-Year Plan for National Technological Innovation, the Special Campaign on Advancing Innovative Development of Intelligent Hardware Industry, and the 13th Five-Year Plan on Developing Emerging Sectors of Strategic Importance (Deloitte 2019).

China's State Council issued the New Generation Artificial Intelligence Development Plan in July 2017, which comprises much of China's AI strategy. The plan aims to accelerate innovation in the area to make China's artificial intelligence field internationally competitive by 2020 and to become a world leader by 2030. At the end of 2017, China detailed some of these goals in the Three-Year Action Plan on Promoting the Development of New Generation AI Industry. Local governments across the country have also issued their own policies detailing how they will enhance AI development.

China's 2019 defense white paper, "China's National Defense in the New Era," states that new technologies can increasingly be applied to the military sphere and that military-civil fusion can work toward modernizing China's military forces.[26]

Proposals to find firmer ground. One of the biggest issues in the U.S.-China relationship regarding artificial intelligence is whether AI-based applications can be used to automate lethal actions. While China has expressed the desire to ban the use of automated lethal weapons, the U.S. has refused to negotiate a new international agreement on autonomous weapons.[27] In addition, neither country has committed to ending the development of such technologies, since they view maintaining artificial intelligence capabilities as essential to winning future wars.

However, China has taken steps toward creating ethical standards in AI. China's "White Paper on Artificial Intelligence Standardization" published by the Standards Administration of China outlines three principles for the ethical use of AI technologies.[28] These are the principle of human interest, which asserts that AI should benefit human welfare; the principle of liability, which states that there should be accountability for the development and deployment of AI-infused technology systems; and the principle of consistency in rights and responsibilities for commercial entities to protect their intellectual property. Other entities have created their own AI ethics standards, including the Beijing Zhiyuan Artificial Intelligence Research Institute, which established the Artificial Intelligence Ethics and Safety Research Center, putting forward the "Artificial Intelligence Beijing Consensus."[29] In July 2021, the Ministry of Science and Technology laid out the "Ethical Norms for New Generation Artificial Intelligence," which states that AI technologies should respect human rights and privacy.[30]

In the US, ethical standards on AI have been adopted by the Department of Defense.[31] These standards include: requiring responsible development and deployment of AI capabilities among Department of Defense personnel; minimizing unintended bias due to AI capabilities; requiring transparency of AI methodologies and data sources; ensuring reliable AI capabilities that are safe, secure, and effective; and requiring AI capabilities to be governable, preventing unintended consequences and permitting deactivation of deployed systems where necessary.

The U.S. Intelligence Community has also laid out ethics regarding AI. These provide guidance on how to develop and use AI. Ethical standards include respecting the law and protecting civil rights; ensuring AI method and use transparency and accountability; reducing bias; applying human judgment in cases where an action may infringe upon civil liberties; ensuring security and resilience using best practices; and using AI that has been informed by science and technology.

As noted above, however, there are some ethical differences between the Chinese and American approaches to AI use. The difference can be reduced to varying views of human rights and legal enforcement/commitment. On one hand, the United States is primarily concerned with individual rights as codified in the Constitution's Bill of Rights, while China is more focused on the rights and security of the citizenry as a whole as led by the Chinese Communist Party. For example, Americans may view freedom of speech as inviolable, while the Chinese may see this freedom as a threat to social stability. These ethical differences will certainly impact the use of AI in both the civilian and military arenas and must be addressed before they create larger rifts between the two countries.

Perhaps, in this case, the U.S. can recognize China's right to use AI in domestic affairs while restricting China from using the technology in the United States. This suggestion is highly unlikely, however, since the U.S. has already crossed this line by sanctioning China for its treatment of the Uyghur people within China's borders and banning imported products from Xinjiang. China views many ethnic Uyghurs as terrorists and violates their human rights by using vast AI systems to identify and track alleged terrorists. This suggests that the U.S. needs to ask itself additional questions about limits to its ability to enforce American human rights standards in other countries. After the U.S. has crossed China's so-called "bottom line," how far is it able and willing to go to enforce its perspective?

However, neither the Chinese nor the American commitment to international agreements is fully credible. Both nations are likely to breach, reject, and refuse to sign or ratify such agreements if they conflict with domestic interests. International agreements are extremely difficult to enforce. As Koplow (2013) notes, the world's leading international judicial tribunal, the International Court of Justice, does not have jurisdictional power over the United States or China because neither has submitted itself to the court's authority.[32] The United Nations Security Council also holds the power to resolve disputes, but the veto power held by each of its five permanent members, including China and the U.S., guarantees that these members will be protected from adverse findings.

Monitoring systems to understand when AI is used maliciously is also essential. The Defense Advanced Research Projects Agency (DARPA) in the U.S. can detect and disrupt malicious information campaigns.[33]

An eventual goal should be to avoid unintended escalation, but that may be difficult to achieve at the outset given high levels of distrust. An interim goal, given that anything concrete is difficult amid the political climate in both the U.S. and China, could be to establish conditions that open the way for discussions about mechanisms for transparency, confidence-building, and de-escalation. This could be in terms of monitoring, limiting the deployment of particularly escalatory AI technologies, and perhaps the use of hotlines so long as humans are part of the decision-making process. The lead up to Cold War-era arms control talks between Russia and the United States could prove instructive given the early lack of transparency and concerns with escalation, even if it is an imperfect analogy. Nonetheless, everything remains tentative until the political climate is more accepting of forward movement, meaning that informal contact and exploration may be all that can be hoped for at the moment.

Notes:

[1] Laskai, Lorand and Helen Toner. 2019. Can China Grow Its Own AI Tech Base? Chapter in STANFORD-NEW AMERICA DIGICHINA PROJECT AI POLICY AND CHINA Realities of State-Led Development, Special Report No. 1 October 29, 2019, Edited by Graham Webster

[2] Deloitte. 2019. Global artificial intelligence industry white paper, https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-ai-report-en-190927.pdf.

[3] Roberts, Huw, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, Luciano Floridi. 2020. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation, AI and Society (2021) 36:59–77.

[4] See page: https://www.alibabacloud.com/blog/city-brain-now-in-23-cities-in-asia_595479

[5] Sullivan, Ryan. 2021. The U.S., China, and Artificial Intelligence Competition Factors. China Aerospace Studies Institute, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Cyber/2021-10-04%20US%20China%20AI%20Competition%20Factors.pdf?ver=KBcxNomlMXM86FnluuvNEw%3D%3D.

[6] GAO. 2021b. Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks. GAO, June 3, https://www.gao.gov/products/gao-21-518.

[7] Sullivan, Ryan. 2021. The U.S., China, and Artificial Intelligence Competition Factors. China Aerospace Studies Institute, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Cyber/2021-10-04%20US%20China%20AI%20Competition%20Factors.pdf?ver=KBcxNomlMXM86FnluuvNEw%3D%3D.

[8] Eggers, William D., Neha Malik, and Matt Gracie. 2019. Using AI to unleash the power of unstructured government data. Deloitte Insights, January 19, https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/natural-language-processing-examples-in-government-data.html.

[9] Department of Defense. 2008. Executive Order 12333 United States Intelligence Activities, Department of Defense, https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf.

[10] Horowitz, Michael C., Gregory C. Allen, Elsa B. Kania, and Paul Scharre. 2018. Strategic Competition in an Era of Artificial Intelligence. CNAS Paper, https://www.indexinvestor.com/resources/Research-Materials/NatSec/Strategic_Competition_in_Era_of_AI.pdf.

[11] Medin, Milo and Gilman Louie. The 5G Ecosystem: Risks & Opportunities for DoD Defense Innovation Board, 3 April 2019. https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF

[12] National Security Commission on Artificial Intelligence. 2021. Final Report, National Security Commission on Artificial Intelligence, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

[13] Temple-Raston, Diana. 2021. China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying, NPR, August 26. https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying

[14] Taipei Times. 2021. Task force at work to combat Chinese deepfake videos. Taipei Times, November 4, https://www.taipeitimes.com/News/taiwan/archives/2021/11/04/2003767291.

[15] Xinhua. 2021. Zhao Lijian said the United States is the world's largest source of cyber attacks, Xinhua, July 20, http://www.xinhuanet.com/world/2021-07/20/c_1127674897.htm

[16] Kania, Elsa. 2018. China’s Strategic Ambiguity and Shifting Approach to Lethal Autonomous Weapons Systems. Lawfare Blog, April 17, https://www.lawfareblog.com/chinas-strategic-ambiguity-and-shifting-approach-lethal-autonomous-weapons-systems.

[17] Congressional Research Service. 2020. Artificial Intelligence and National Security Updated November 10, 2020 , Congressional Research Service Report, https://fas.org/sgp/crs/natsec/R45178.pdf.

[18] Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima, Derek Grossman. 2020. Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World, RAND Research Publication, https://www.rand.org/pubs/research_reports/RR3139-1.html.

[19] Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima, Derek Grossman. 2020. Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World, RAND Research Publication, https://www.rand.org/pubs/research_reports/RR3139-1.html.

[20] White House. 2022. “FACT SHEET: Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public,” October, White House, https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/

[21] AI.gov. 2022. AI.gov National AI Initiative Act. AI.gov, accessed September 28, https://www.ai.gov/#:~:text=The%20National%20AI%20Initiative%20Act,economic%20prosperity%20and%20national%20security.

[22] National Science and Technology Council. 2019. The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update. A Report by the Select Committee on Artificial Intelligence of the National Science and Technology Council, June, https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf.

[23] Congressional Research Service. 2020. Artificial Intelligence and National Security Updated November 10, 2020 , Congressional Research Service Report, https://fas.org/sgp/crs/natsec/R45178.pdf.

[24] National Security Commission on Artificial Intelligence. 2021. Final Report, National Security Commission on Artificial Intelligence, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

[25] Sheehan, Matt. 2022. China’s New AI Governance Initiatives Shouldn’t Be Ignored, January 4, Carnegie Endowment, https://carnegieendowment.org/2022/01/04/china-s-new-ai-governance-initiatives-shouldn-t-be-ignored-pub-86127

[26] Uber, Maj. Richard. 2020. China's Artificial Intelligence Ecosystem. NIU Research Monograph, https://ni-u.edu/wp/wp-content/uploads/2021/08/Uber_Monograph_DNI2021_02261.pdf.

[27] Wareham, Mary. 2018. Campaign to Stop Killer Robots: Report on Activities, Convention on Conventional Weapons Group of Governmental Experts meeting on lethal autonomous weapons systems United Nations, Geneva, 9-13 April 2018.

[28] Ding Jeffrey, Triolo Paul (2018) Translation: excerpts from China's "White Paper on Artificial Intelligence Standardization." New America. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-excerpts-chinas-white-paper-artificial-intelligence-standardization/.

[29] Sun, Mingchun. 2021. Ethical norms and industry self-discipline in the development of artificial intelligence technology (in Chinese), Sina news, January 14, https://finance.sina.com.cn/tech/2021-01-14/doc-ikftpnnx6825029.shtml.

[30] Georgetown University Center for Security and New Technology. 2021. Ethical Norms for New Generation Artificial Intelligence Released, Georgetown University Center for Security and New Technology. October 21, https://cset.georgetown.edu/publication/ethical-norms-for-new-generation-artificial-intelligence-released/

[31] Department of Defense 2020. DOD Adopts Ethical Principles for Artificial Intelligence, Department of Defense website, February 24, https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

[32] David A. Koplow. 2013. Indisputable Violations: What Happens When the United States Unambiguously Breaches a Treaty, Fletcher Forum of World Affairs 37(1): 53-74.

[33] National Security Commission on Artificial Intelligence. 2021. Final Report, National Security Commission on Artificial Intelligence, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

V. Internet of Things

The technology and its uses. The Internet of Things refers to the network of billions of objects worldwide that are connected to the internet. These objects contain chips and often sensors that send data back to databases for analysis. They include wearable devices, auto parts, household appliances, and medical devices.

The Internet of Things can be used for both civilian and military purposes. IoT is increasingly incorporated into the construction of smart cities, which can improve residential services, transportation, and public utilities. Smart schools can help track attendance and meal payments, while utilities can take advantage of smart lighting and smart meters. Intelligent transportation systems and smart parking can help increase public transportation efficiency. Even so, looking at individual cities, there were no U.S. or Chinese cities among the top 10 cities of the IMD Smart Cities Index for 2021.[1]

Additionally, IoT is used for military purposes to make up for workforce challenges. Creating a warfighting network makes for speedier intelligence collection and threat identification. This process includes collecting data through sensors on numerous platforms, such as weapon systems, aircraft, and troops. The IoT-connected sensors and radars collect and transmit data on the positioning and movement of U.S. troops and countries of interest.[2]

Application of IoT lags in other areas in the U.S., including within the federal government. The U.S. Government Accountability Office found that while many federal agencies use IoT to monitor equipment, control facility access, or track physical assets, agencies that did not intend to use IoT viewed such devices as having low returns.[3] While some agencies use IoT, their application mainly focuses on specific objects rather than on an IoT ecosystem and, more significantly, automated decision-making or data analysis.

On balance, China assesses that the IoT has a higher value in streamlining public services than the U.S. China is building up urban IoT infrastructure, as directed by several central government departments. This infrastructure seeks to accelerate IoT infrastructure by 2023, setting up IoT demonstration bases, digital villages, smart transportation, smart construction, and smart agriculture by 2023.[4] This method is far ahead of U.S. government implementation or planning.

The NATO Science and Technology Committee report on the Internet of Things finds that this technology has great potential in military applications[5]. IoT devices can be used in sensors for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems to gather and transmit data. Additionally, the IoT can be used for firepower control systems to respond automatically to threats. Mobile technologies applied to IoT devices, such as smartphones, can provide access to tracking or mapping applications. IoT devices can also track shipments and log movements within logistics systems.

However, there are many vulnerabilities associated with the IoT. The increased connectivity of IoT devices may lead to congestion across networks, which could block the functionality of critical devices, such as medical devices. Malicious network attacks can also lead to device malfunctions, which could be costly to human life or critical infrastructure. Russia's invasion of Ukraine showcases that the IoT can be a vehicle for information warfare. Against the backdrop of financial sanctions from the U.S., Canada, and the European Union, hackers have employed cyberattacks to combat Russia. Anonymous, a hacker group, has declared a cyberwar on Russia by hacking stream services.[6]

IoT also increases the potential cyber-attack and cyber-accident surface, rendering new vulnerabilities where there were fewer or different vulnerabilities before. The power, telecom, and IT industries may be critical as attacking these industries would have significant negative consequences. With the growth of 5G and artificial intelligence, there is an increased possibility of attacks on IoT devices. Both technologies speed up the rate at which attacks could occur, increasing the likelihood of success within any given timeframe. 6G looms large as China has already begun working on the infrastructure, while the U.S. is still overcoming security challenges from an unstable 5G rollout.

The concern for the U.S. is that the global power that controls 6G will command the rest of the century. 6G would be used in military operations and our day-to-day lives. Currently, China enjoys unprecedented influence on the global stage regarding the diffusion and deployment of advanced communications technologies. 6G would have an air latency of less than 100 microseconds and is expected to be 100 times faster than 5G, with broader network coverage and enhanced reliability. With the implementation of 6G-based solutions, IoT will continue to become increasingly integrated into people's lives and connect 10 times more devices per square kilometer and significantly more connected devices to come.[7]

Concerning military applications, the benefits of IoT that beneficially transform modern warfare are also causing concern about malicious cyberattacks. The tremendous impact of IoT is the increase of available methods and opportunities for data gathering, yet the trouble is that hackers can also take advantage. Concerns include vehicle safety, healthcare, and supply chains. Hackers could commandeer vehicles, take control of medical devices, and disrupt supply chain operations. In addition, IoT devices may provide hackers with critical information. In March 2021, hackers gained access to Silicon Valley's Verkada Inc., infiltrating companies', hospitals', prisons', schools', and police departments' live feeds that included 150,000 surveillance cameras. Hackers viewed videos from psychiatric hospitals and Verkada's offices.[8]

There is also a concern in the U.S. that China will set international standards for IoT devices. This trend would allow China to use IoT more effectively for surveillance and collecting intelligence. A report prepared for the U.S.-China Economic and Security Review Commission stated that "the combination of widespread adoption of IoT products and Chinese research into exploits raises the threat of unauthorized access to U.S.-based IoT devices and the networks they connect to."[9] The authors assert that IoT devices manufactured in China are targets for exploitation.

Another issue underscored in the U.S.-China Economic and Security Review Commission report is that the IoT contains many different devices and systems with multiple providers of endpoints, gateways, and networks. The systems require compatible standards so that product designers and consumers will be able to purchase and use devices interchangeably.

To some extent, the issue between the U.S. and China on IoT stems from the fact that China has had streamlined policies to integrate IoT into everyday life across a variety of industries. China is ahead in this area, which gives the country an edge in using the technology to serve its own purposes. China uses the IoT in smart cities for real-time data collection, in industry to optimize operations, in medicine to improve patient care and collect medical data, and in smart cars to sense how vehicles relate to the road environment. As a result, the U.S. would benefit from policies that furthered technology in this area as well so that it can remain competitive.

Current policies. In the U.S., recent policy has increased IoT security at the federal level. Recently, Congress approved the Strengthening American Cybersecurity Act of 2022. This act covers critical infrastructure and the federal government. It includes mandatory cyber incident reporting by owners of critical infrastructure within a specified time frame of a cyber breach. Despite the passing of this legislation, cyber incident reporting is often complicated because of the incentives behind choosing not to report and the differences between what is reported to the government and to the public.[10] Existing reporting regulations are too narrow and insufficiently standardized. For example, in 2015, the Office of Personnel Management was hacked, negatively impacting about 22 million personnel records. This breach took place in June but was not reported until April due to a lack of reporting regulations and standards. The 2022 act's cyber incident report requires reporting from critical infrastructure owners four days from the breach. Timely reporting on cyber incidents assists with faster responses.

The IoT Cybersecurity Improvement Act also became law at the end of 2020. This act required the National Institute of Standards and Technology (NIST) and the Office of Management and Budget to raise cybersecurity for the IoT devices among federal agencies, including creating and producing standards and guidelines for the government on best practices to ensure that principles and policies are consistent with NIST's standards and guidelines.[11]

Chinese focus on IoT began in 2009 with the inclusion of the sector in Premier Wen Jiabao's work report as one of five "strategic emerging industries." The State Council's 2010 decision on strategic new emerging industries also promoted IoT. MIIT and the National Development and Reform Commission have laid out tasks and priorities for IoT development. State and local departments have rolled out policies promoting IoT development.[12]

With regard to IoT, the U.S. has prevented sale of critical technologies to China to maintain its technological prowess. The Obama administration in 2015 prevented Intel, Nvidia, and Advanced Micro Devices from selling highly sophisticated supercomputer chips to China to avert their use in military devices. Two years later, in 2017, the Trump administration barred the sale of the Lattice Semiconductor, which holds programmable software that provides an alternative way to build AI chips, to a Chinese-backed investor.[13] In 2022, the Biden administration banned advanced semiconductor technology exports to China.

The Committee on Foreign Investment in the United States (CFIUS), which recommended that the sale of Lattice be blocked, helps to protect strategically important technologies. CFIUS' ability to review foreign investments was expanded under the Foreign Investment Risk Review Modernization Act of 2018.

In addition, in May 2019, President Donald Trump issued an executive order that banned U.S. companies from using information and communications technology from companies considered a national security threat. As Huawei's products were judged to be insecure, it was added to the entity list by the Commerce Department the same day. In June, the U.S. added five other companies, including Chengdu Haiguang Integrated Circuit, Chengdu Haiguang Microelectronics Technology, Higon, Sugon, and Wuxi Jiangnan Institute of Computing Technology.

President Joe Biden has extended this policy and included more firms on the entity list. These companies include Aviation Industry Corporation of China, Proven Glory Capital, and Proven Honour Capital, which have served as financial arms of Huawei and sold bonds to international investors.[14] The Commerce Department also added a substantial number of Chinese military-related research institutes and companies to the entity list, including the Academy of Military Medical Sciences and 11 research institutes in response to emerging technologies for "brain-control" weapons. Chinese military-civil fusion, or MCF, is the Chinese government's strategy to reach its goal to create the most technologically advanced military in the world. Entities that produce biotechnologies supporting China's MCF strategy were also placed on the entity list. Furthermore, in response to China's human rights violations in Xinjiang, the Biden administration added a substantial number of related entities to a U.S. investment blacklist. These entities include SenseTime, China's top artificial intelligence firm, identified as developing facial recognition programs to track Uyghurs.[15]

Proposals to find firmer ground. The U.S. and China both need to recognize that the Internet of Things remains vulnerable to exploitation and needs to be further secured. Rules and standards in both countries should increase the security of such devices, and network-scanning software should be updated to notify owners of intrusions. Consumer privacy rules must be applied to IoT devices to limit sensitive data collected, and IoT devices should disclose potential data exposure issues.

China already has some regulations to protect privacy rights against IoT devices. The Measures for the Protection of Information Security Levels contain five security levels for information and data management systems. IoT devices that collect customer data fall under this regulation.

Standardization, in general, can also help to ensure that neither the U.S. nor China is locked out of participation in the other country’s markets due to incompatible systems. International standardization bodies can help to bring together national standards-setting departments. Within the U.S. government, a department needs to be responsible for developing IoT or 5G standards within America. By contrast, China has expanded its standardization work by focusing on modernization and standardization of industry through its 2018 revised Standardization Law and China Standards 2035 project.

Notes:

[1] IMD. 2021. Smart City Index 2021. IMD publication, https://www.imd.org/smart-city-observatory/home/.

[2] Lockheed Martin. 2017. IOT is Transforming Modern Warfare, Lockheed Martin website, https://www.lockheedmartin.com/en-us/news/features/2017/internet-of-things-transofrming-modern-warfare.html

[3] GAO. 2020. Internet of Things: Information on Use by Federal Agencies. GAO Report GAO-20-577, https://www.gao.gov/assets/gao-20-577.pdf.

[4] Ministry of Industry and Information Technology. 2021. Notice on Printing and Distributing the "Three-year Action Plan for the Construction of New Internet of Things Infrastructure (2021-2023)." Ministry of Industry and Information Technology Notice [2021] No. 130, http://www.gov.cn/zhengce/zhengceku/2021-09/29/content_5640204.htm.

[5] Tonin, Matej. 2017. The Internet of Things: Promises and Perils of a Disruptive Technology. NATO Science and Technology Committee Report, https://www.nato-pa.int/download-file?filename=/sites/default/files/2017-11/2017%20-%20175%20STCTTS%2017%20E%20bis%20-%20INTERNET%20OF%20THINGS.pdf.

[6] Dan Milmo. 2022. Anonymous: the hacker collective that has declared cyberwar on Russia, The Guardian, February 27, https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

[7] Qadir et al. 2022. Towards 6G Internet of Things: Recent advances, use cases, and open challenges. ICT Express, https://www.sciencedirect.com/science/article/pii/S2405959522000959

[8] Horowitz, Michael C., Gregory C. Allen, Elsa B. Kania, and Paul Scharre. 2018. Strategic Competition in an Era of Artificial Intelligence. CNAS Paper, https://www.indexinvestor.com/resources/Research-Materials/NatSec/Strategic_Competition_in_Era_of_AI.pdf.

[9] John Chen, Emily Walz, Brian Lafferty, Joe McReynolds, Kieran Green, Jonathan Ray, and James Mulvenon. 2018. China's Internet of Things, Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission October 2018, https://www.uscc.gov/sites/default/files/Research/SOSi_China's%20Internet%20of%20Things.pdf

[10] Mary Brooks, Sofia Lesmes. 2022. Last Call at the "Star Wars Bar": Harmonizing Incident and Breach Reporting Requirements, Lawfare Blog, July 5, https://www.lawfareblog.com/last-call-star-wars-bar-harmonizing-incident-and-breach-reporting-requirements

[11] Scott Ikeda. 2020. IoT Cybersecurity Improvement Act Signed Into Law: New Security Requirements for Federal Government Devices, CPO Magazine, December 18, https://www.cpomagazine.com/cyber-security/iot-cybersecurity-improvement-act-signed-into-law-new-security-requirements-for-federal-government-devices/

[12] Lee, John. 2021. The Connection of Everything: China and the Internet of Things, MERICS report, June 24, https://merics.org/en/report/connection-everything-china-and-internet-things.

[13] Wang You and Chen Dingding. 2018. Rising Sino-U.S. Competition in Artificial Intelligence, China Quarterly of International Strategic Studies, Vol. 4, No. 2, 241–258

[14] Jennifer Jacobs. 2021. Biden blocks 59 Chinese companies including Huawei in amended Trump order, Business Standard, June 4. https://www.business-standard.com/article/international/biden-blocks-59-chinese-companies-including-huawei-in-amended-trump-order-121060400185_1.html

[15] Jeanne Whalen. 2021. U.S. bans investment in Chinese surveillance company SenseTime, saying it supports repression of Uyghur minority population, Washington Post, December 10, https://www.washingtonpost.com/technology/2021/12/10/us-investment-ban-sensetime/

VI. Big Data and Privacy

The technology and its uses. Big data refers to massive data sets that can be analyzed to reveal otherwise undiscovered patterns and associations. Big data tends to be generated at high volumes per second across a large variety of data types. Such large amounts of data can then be used to better determine customer preferences, supply chains, or market risks. Larger amounts of data, particularly coupled with faster processing speed and technologies such as artificial intelligence and cloud computing, result in better understanding of patterns that indicate everything from customer creditworthiness or market trends to more efficient design of roads and logistic chains.

Big data may be subject to attack in various ways. For example, the Hadoop framework, which is a commonly used platform for big data, has known vulnerabilities that must be closed to reduce the risk and damage of cyberattacks. The framework was initially built without strong security considerations, and security was patched on in later versions. Hadoop's weak points include potential for password leakage to particular applications, user or group information storage corruption, denial of service issues, user account impersonation, and more. As many institutions use Hadoop, this creates serious concerns over data security. The threat is compounded by the fact that lists of companies using Hadoop are available over the internet. Other big data frameworks face similar issues.

Data privacy is an issue that was amplified during the Trump years, particularly among technology companies that collect and process big data. The Trump administration attempted to ban Chinese social media company Tiktok in the United States, as well as to restrict operations of WeChat and Alipay over fears of Chinese data access. According to Samm Sacks (2020), the issue of data privacy between the United States and China is complex in part because the U.S. lacks a comprehensive data privacy regulation that addresses the issues.[1]

Among the targets for hacking in the U.S. have been large troves of personal data, which may reveal exploitable individual vulnerabilities. These include the exfiltration of personal data on federal employees from the U.S. Office of Personnel Management in 2015 in addition to hacks on health insurance firms, tax preparation companies, and hotel chains that provide a huge trove of data.[2] Access to such data, which can then be analyzed using artificial intelligence, can enable actors to target key personnel and compromise them by identifying personal weaknesses.[3] One reason such vulnerabilities exist is inadequate protections on big data in the United States, a problem that persists despite scandals over the collection and use of big data from Facebook by Cambridge Analytica.[4]

China, too, worries about data privacy, albeit relating to the collection and storage of data by commercial entities. For example, a Reuters report from November 2021 states that the Cyberspace Administration of China sought a delisting of the ride-hailing app company Didi from the U.S. stock market due to data security concerns.[5] This move may have to do with the significant amounts of personal data such apps store, potentially including information from state sources. A November 2021 report by Now from Hong Kong revealed that a dating app was able to retrieve personal information about individuals from the Public Security Bureau.[6] A concern for the Chinese state is addressing what they see as the potential for foreign espionage, cyberattacks, and malign collection and manipulation of data.

Both the United States and China have entities that collect large amounts of individual social media data, which can affect personal privacy and even subject individuals to harassment. Such efforts tend to be state-related in China and associated with profit-making enterprises and elections in the United States, though state-related efforts in China do also have commercial tie-ups and applications. Recent investigative reports point to China-related entities collecting large amounts of social media information relating to policymakers, academics, and others of interest to the state.[7] Chinese security agencies are also allegedly collecting information on social media accounts to silence critics online, including to intimidate family members.[8] With regard to the U.S., Cambridge Analytica represents the most prominent example of data collected on individual social media accounts in support of disinformation relating to election campaigns.[9] Whistleblower accounts detail Facebook and other social media companies extracting user data to drive advertising profits, even to the detriment of users.[10] Security flaws further complicate risks from such activities.

Even if the Chinese state collects and manages large amounts of data on individuals, it is more ambivalent about giving commercial entities greater access, as seen in the passage and implementation of Personal Information Protection and Data Security laws in 2021.[11] Under the Data Security Law, data from China must be stored locally rather than in overseas servers consistent with its insistence on cyber sovereignty. Like many Chinese laws, these new pieces of legislation give the state significant remit. Violations can result in hefty fines and blacklisting for corporations.[12] That said, these laws are consistent with rising public concerns about data privacy in relation to commercial interests among Chinese citizens (Liu, 2020).

Common concerns about big data and data privacy in the hands of commercial entities may, therefore, provide some grounds for U.S.-China cooperation. Despite a lack of coordinated regulation and resistance by social media firms, there appears to be a growing momentum in the United States for more regulation on the data that corporations can collect and store in the wake of the latest scandal facing Facebook/Meta.[3] There may be some basis for Washington and Beijing to come up with common standards of regulating commercial use of big data given shared skepticism toward the power that such information provides to corporations. Limiting what commercial firms collect and store can also reduce security risks for both the United States and China. Washington and Beijing can further work with the European Union, which had earlier put forward their General Data Protection Regulation (GDPR) to begin addressing some of these issues, including the right to erasure.[14]

Current policies. China's cybersecurity policies are governed by the Cybersecurity Law of the People's Republic of China, which establishes obligations of internet service providers, personal information protection, and information infrastructure security. China also has other regulations, including the Information Security Technology — Implementation Guide for Classified Protection of Information System and the Information Security Technology — Classification Guide for Classified Protection of Cybersecurity. China's data regime is protected by the Cybersecurity Law, which came into effect in June 2017. The Cybersecurity Law aims to protect citizens and organizations in the cybersecurity realm. An underlying consideration of the Chinese approach toward online information and privacy is the concept of cyber sovereignty, where the state should have control of all information generated and used within its jurisdiction, including citizens and corporations abroad (Creemers, 2020).

China's Personal Information Protection Law (PIPL) provides a degree of online privacy protection vis-à-vis commercial entities. PIPL limits the data that corporations can collect on individuals, including consent, access, rectification, and erasure, while restricting the transfer of individual data outside of China's borders. This includes corporate human resources data such as employees' compensation and performance data. Like Europe's GDPR, PIPL provides extraterritorial jurisdiction to the Chinese state, affecting not only corporations with a physical presence in China but also those that conduct business with entities located in China. Unlike the GDPR, however, PIPL neither restricts nor provides oversight of state action. PIPL also has no mandates on the safe destruction of data.

The related Data Security Law regulates the processing and transfer of data overseas. It does so by categorizing different levels of data. Most strictly controlled is "core" data pertaining to national interests, followed by "important" data that includes information relating to national interests and individuals. Any transfer of such data overseas, including the handing over of data to foreign law enforcement agencies and judiciaries, requires differing levels of official approval. Generally, any personal or consumer data collected in China must be stored within China and not transferred abroad. Like PIPL, the Data Security Law has extraterritorial reach, again meaning that commercial entities that do business with individuals and businesses in China are subject to these regulations even if they do not have a physical or legal presence within China.

The U.S. does not have an all-encompassing data protection law, relying on a combination of federal and state laws to protect privacy. The Federal Trade Commission Act allows the U.S. Federal Trade Commission to bring actions against firms that engage in unfair or deceptive data privacy activities or that fail to provide sufficient security of personal information. Federal sector-specific laws also strive to protect personal data privacy. State laws may restrict use of personal data as well. Congressional testimony over Facebook/Meta's use of user data is currently fueling discussion on a need for legislation to further regulate the collection and use of personal data available on social media.

Data privacy is an issue that is gaining greater public attention in the United States, but there remains no comprehensive legislative or policy approach parallel to China's PIPL and Data Security Law or the European Union's GDPR. Public awareness of the risks surrounding data privacy increased dramatically with the scandal surrounding the sale and use of Facebook data by the firm Cambridge Analytica to influence both the United Kingdom's Brexit referendum and the 2016 U.S. presidential election. The matter gained further public traction with the growth in popularity of Chinese-owned social media service TikTok and leaks by Facebook/Meta whistleblower Frances Haugen. Nonetheless, legislative and policy responses are piecemeal at present, opening the United States to espionage risks and U.S. citizens to cybercrime as well as excessive corporate manipulation of their personal data.

Common concerns in both Washington and Beijing about the collection and exploitation of user data may provide some basis for cooperation between the two sides. Washington likely has reason to protect users from harassment and risks from state actors like China and Russia as well as exploitation and misuse by technology firms like Facebook/Meta and TikTok/ByteDance. Beijing has a desire to prevent external state and corporate actors from accessing personal data about its citizens and companies under its concept of cyber sovereignty. This confluence of interests provides some grounds for discussion, confidence-building, and even coordination between Washington and Beijing over regulation of the collection, sharing, and storage of personal and corporate information on social media and other platforms. Even if the United States and China initially embark on unilateral efforts to regulate these areas, their convergence of interests on such issues may provide future opportunities for seeking understanding.

Cyberattacks. In an environment of increasing political tension, the potential for future U.S.-China cyberconflict is on the rise. Some experts have commented that the

U.S.-China new technology rivalry looks like a “digital cold war.”[15] However, at present, much of the conflict between the two nations appears to be in the area of politics and trade, and cyberconflict has not been a major focus.

The U.S.-China technology rivalry has been characterized as a type of cold war because there is no “opting out” of new technologies for either country. If either the U.S. or China spends much of its time maintaining mature systems without investing in new systems, that country will lose any technology and security advantage it might have had. Utilization of new technology is essential, as are funding for research and development and policies to promote implementation.

As new technologies are increasingly implemented, the potential for cyberconflict will inevitably grow. One reason for this is that new technologies create new vulnerabilities. AI and 5G in particular will greatly expand the number of feasible cyberattack surfaces. Another reason is that new technologies can be adapted for malicious purposes.
To some extent, China is less vulnerable than the U.S. because China has a limited number of ports through which the domestic internet is connected to international networks. This means that China could shield itself more readily from large-scale cyberattacks. China’s media is also heavily controlled, increasing the possibility for third parties to spot content-related security hacks as well as reducing citizen sensitivity to government intervention in new technologies.

Both nations have cybersecurity units as part of national defense departments. For example, the U.S. set up a Cyber Command in 2009 to combat cyberattacks and has used numerous cyberwarfare tactics in physical conflicts. China’s Third Department of the People’s Liberation Army consists of cybersecurity forces, and the People’s Liberation Army includes computer network operations as part of its military operations.

The U.S. and China have so far not been engaged in a cyberwar per se, but the two countries have been involved in cyberconflict. Cyberwar can be defined as attack and defense on and of computer systems, including hardware and/or software, while cyberconflict may constitute smaller acts of aggression that do not escalate to the scale and intensity of a cyberwar.

Both sides have participated in cyberconflict, however. The U.S. allegedly originates most offensive cyberattacks on China. A report by China’s National Computer Network Emergency Response Technical Team (CNERTT) found that there was a 91% increase in cyberattacks by the U.S. on China in 2018, infecting 3,607 Chinese websites.[16] The U.S. often seeks information related to military and government organizations through cyberattacks, and the U.S. National Security Agency regularly spies on Chinese computers and networks.

That said, CNERTT does not appear to clearly distinguish between state-related and non-state cyberattacks on China that may originate from the United States.

Under the Obama administration, Chinese hacking of the U.S. declined markedly due to a bilateral agreement in 2015 to stop hacking intended to steal trade secrets. Hacking picked up again under the hawkish Trump administration, which issued a report by the U.S. Trade Representative in March 2018 detailing cases of Chinese cybertheft against the United States.[17] At the end of 2018, China stepped up cyberattacks on U.S. critical infrastructure in the areas of energy, financial, transportation, and healthcare (Finkle and Bing 2018). Most of the cyberattacks, however, were focused on stealing technological secrets. In response to Chinese cyberattacks, the U.S. has been carrying out counter-cyberattacks against Chinese intelligence and military targets. In addition, Zhu Hua and Zhang Shilong, two Chinese nationals, were accused of participating in hacking campaigns that targeted several U.S. government agencies, including the Energy Department, laboratories at NASA, and the U.S. Navy. International Business Machines Corp. and Hewlett Packard Enterprise Co. are among companies whose computer-services operations were breached by hackers, who then used that access to burrow into their clients' networks. China's hacking campaign allegedly aimed to target technology services providers that support businesses with technologies such as cloud storage.

In 2021, a major hack of Microsoft Exchange servers that U.S. officials and experts attributed to China may represent a return to more aggressive cyberattacks, but the aim of the attack may be to build up a database of personal information of Americans rather than just commercial.[18] In 2022, it was reported by Chinese media that the U.S. National Security Agency infiltrated China's telecommunications networks. The Global Times, a state media outlet, asserted that the U.S. stole key technology data, such as network equipment configuration, network management data, and operational data.[19]

Recent U.S. policy has improved the ability of the U.S. to respond to cyberattacks. The Presidential Policy Directive 41 of July 2016 dictates a federal response to cyberattacks to either the public or private sectors. A May 2017 executive order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," states that the executive branch has the authority to control cybersecurity risk for critical infrastructure. The order notes that the government will respond rapidly to attacks in collaboration with the private sector. In addition, in 2018, U.S. President Trump reversed President Obama's Presidential Policy Directive 20 under the classified National Security Presidential Memorandum 13, which allows the U.S. government to use powerful cyber weapons.

The stakes of becoming a cyberattack victim are high for both nations, especially regarding critical infrastructure. Therefore implementation of cybersecurity must be viewed as equally important to implementation of new technologies at the micro-level. In addition, it is essential that new technology firms and industries gain protection from external use and exploitation. In some cases, only the government can block transactions that could threaten pioneering new technology industries.

Despite the rising stakes of cyberconflict and the conflict-ridden political environment, the best bet either country has at reducing the possibility of conflict is to work together. Improved relations can deter the regular use of damaging cyberattacks between the U.S. and China by increasing the costs associated with such behavior.

We recommend that the U.S. set up a coordinated effort to enhance cybersecurity by protecting networks, databases, the Internet of Things, and other critical technology infrastructure. We also recommend that the U.S. set up an ongoing dialogue with China to address cybersecurity issues between the two countries that also covers data collection, storage, and use. Big data, after all, is becoming an increasingly common target for cyberattacks and can be exploited to compromise both commercial and security interests. Finally, we recommend the creation of a new global governance institution that can address cyberconflict and help to ensure cyber peace.

The diplomatic component to maintaining peace in cyberspace cannot be stressed enough. High-level negotiation has been shown to be effective in deterring Chinese hackers from attacking U.S. targets under the Obama administration and, even more importantly, has played a major role in building up U.S.-Chinese political and economic relations over the past 40 years. The U.S. and China should make better use of the High-Level Joint Dialogue on Cybercrime and Related Issues and the Law Enforcement and Cybersecurity Dialogue, engaging military leaders in the process as well.

Proposals for finding firmer ground. The U.S. needs to implement data rules for all firms, both domestic and foreign, without blocking data flows to the U.S. Regulations must take into account national security and privacy concerns, considering the extent to which data collected is sensitive or risky and how the data is used. A federal data privacy law would address these issues as well as cross-border data flows and collection and storage of personal information by foreign firms. This would reduce the focus on China as a strategic competitor and create a more systematic and rational means of treating data usage. Without a clearer sense of standards on the U.S. side, trying to move forward on trying to establish some sort of understanding with other actors, including China, would be highly challenging.

The U.S. and China, along with the European Union, share interests in the regulation of big data and privacy protection. Publics in these jurisdictions demand limits on how and to what extent their personal data can be used for commercial purposes beyond their original intention. Such commonality provides some basis for cooperation or at least coordination on regulating the types of data that commercial entities can collect, store, transfer, use, and sell, as well as establishing protocols for consent and the safe destruction of commercially held data. There is likely to be resistance in the United States from technology firms whose business models rely heavily on harvesting, using, and selling personal data. However, mobilizing public support to overcome lobbying efforts should be possible.

Collaboration on these matters by the United States, China, Europe, and others can afford the public better protection of privacy while limiting the exposure of states and corporations to espionage risks. Even if such regulation restricts what any individual state can exploit regarding adversaries, competitors, and rivals, they can take away an element of contestation and reduce friction. Governments have an interest to move forward on better privacy protections regarding big data, at least in the commercial realm. Indeed, this is what the European Union and China have done with recent legislation. The United States should follow suit, especially given that models from which to take reference now exist, such as the European Union's GDPR.

There should also be thinking about how to relate discussions about big data and privacy to cybersecurity, which are two distinct but linked issues. Ongoing dialogue with China to address cybersecurity issues between the two countries should also cover data collection, storage, and use. Big data, after all, is becoming an increasingly common target for cyberattacks and can be exploited to compromise both commercial and security interests. There should be some coverage of cybercrime as well, given the persistent risk of states working with cybercriminals to engage in cyberattacks.

However, there needs to be recognition that the United States and Europe view data and privacy in a way that is fundamentally different from China. Like Russia, China holds a commitment to cyber sovereignty.[20] All information generated within the state belongs to the state. This can extend to its citizens and companies operating overseas. The U.S. and Europe tend to believe in a need to keep information from the prying eyes of the state, even if this sometimes means not scrutinizing corporations sufficiently.

Such basic philosophical differences in thinking undergird legal frameworks in the United States and China and need to be accounted for in any discussion on data and privacy. A possible way forward may be to focus first on areas of agreement — such as the need to protect data — as a basis to build trust before moving on to more difficult topics. Coordination on this front can be technical and less potentially contentious since both Washington and Beijing have an enduring interest in protecting their public as well as private data.

Notes:

[1] Samm Sacks. 2020. Data Security and U.S.-China Tech Entanglement. Lawfare Blog, April 2, https://www.lawfareblog.com/data-security-and-U.S.-China-tech-entanglement.

[2] Adams, Michael. 2016. Why the OPM Hack is Far Worse than You Imagine. Lawfare Blog, March 11, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine; Graff, Garrett M. 2020. China's Hacking Spree will Have a Decades-Long Fallout. Wired. November 2, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/; Peterson, Andrea. 2015. 2015 is Already the Year of the Healthcare Hack--and It's Only Going to Get Worse. Washington Post, March 20, https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/

[3] Temple-Raston, Diana. 2021. China's Microsoft Hack May Have Had a Bigger Purpose Than Just Spying, NPR, August 26. https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying

[4] Fruhlinger, Josh. 2020. The OPM Hack Explained: Bad Security Practices Meet China's Captain America. CSO Online, February 12, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html; Lapowski, Issie. 2019. How Cambridge Analytica Sparked the Great Privacy Awakening. Wired, March 17, https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/

[5] Zhu, Julie, Kane Wu, and Brenda Goh. 2021. Beijing Presses Didi to Delist from U.S. Over Data Security Fears -- Sources. Reuters. November 26, https://www.reuters.com/world/china/china-asks-didi-delist-us-security-fears-bloomberg-news-2021-11-26/

[6] Now新聞. 2021. 「交友網站經過大數據配對 連接公安系統認證身份」. 《Now新聞》, November 19, https://news.now.com/home/local/player?newsId=457163

[7] Cate Cadill. 2021. China Harvests Masses of Data on Western Targets, Documents Show. Washington Post, December 31, https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html

[8] Xiao, Muyi and Paul Mozur. 2021. A Digital Manhunt: How Chinese Police Track Critics on Twitter and Facebook. The New York Times, December 31, https://www.nytimes.com/2021/12/31/business/china-internet-police-twitter.html?referringSource=articleShare

[9] Hern, Alex. 2018. Cambridge Analytica: How Did It Turn Clicks into Votes? The Guardian, May 6, https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

[10] Morris, Loveday, Elizabeth Dwoskin, and Hamza Shaban. 2021. Whistleblower Testimony and Facebook Papers Trigger Lawmakers Call for Regulation. Washington Post, October 25, https://www.washingtonpost.com/technology/2021/10/25/facebook-papers-live-updates/

[11] Horwitz, Josh. 2021. China Passes New Personal Data Privacy Law, to Take Effect Nov. 1. Reuters, August 20, https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/

[12] Burgess, Matt. 2021. Ignore China’s New Data Privacy Law at Your Peril. Wired, November 5, https://www.wired.com/story/china-personal-data-law-pipl/

[13] Dan Milmo, 2021. Facebook and Instagram gathering browsing data from under-18s, study says, The Guardian, Nov 16, https://www.theguardian.com/technology/2021/nov/16/facebook-and-instagram-gathering-browsing-data-from-under-18s-study-says

[14] European Union. 2021. What is GDPR, the EU’s New Data Protection Law? GDPR.eu. https://gdpr.eu/what-is-gdpr/.

[15]Marc Champion. Digital Cold War, 2019. Bloomberg Quick Take, December 12, https://www.bloomberg.com/quicktake/how-u-s-china-tech-rivalry-looks-like-a-digital-cold-war

[16] Lindsey, Nicole. 2019. New CNCERT Report Shows Most Cyber Attacks on China Originate from United States, CPO Magazine, June 24, https://www.cpomagazine.com/cyber-security/new-cncert-report-shows-most-cyber-attacks-on-china-originate-from-united-states/

[17] USTR. 2021. U.S.-E.U. Trade and Technology Council (TTC), Accessed December 8, 2021, https://ustr.gov/useuttc

[18] Temple-Raston, Diana. 2021. China's Microsoft Hack May Have Had a Bigger Purpose Than Just Spying, NPR, August 26. https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying

[19] Kharpal, Arjun. 2022. “Chinese state media claims U.S. NSA infiltrated country’s telecommunications networks,” CNBC, September 22, https://www.cnbc.com/2022/09/22/us-nsa-hacked-chinas-telecommunications-networks-state-media-claims.html

[20] Creemers, Rogier. 2020. China’s Approach to Cyber Sovereignty, Konrad Adenauer Stiftung, Berlin, Germany,
https://www.kas.de/documents/252038/7995358/China’s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537

VII. Semiconductors

The technology and its uses. Semiconductors are a foundational technology for virtually all modern electronics. They can be divided into broad categories of application, among which there are different types of integrated circuits (ICs). Examples of ICs used throughout society include processors that provide the “brains” for computers, memory chips that store information, and signal converters that interface between digital and analog signals (for example, converting digital information into sound waves in electronic audio devices). Other types of semiconductors are also becoming increasingly common and in demand, as technology becomes increasingly digitized. Notably, semiconductors are used in sensors, which are increasingly ubiquitous as the Internet of Things expands.

The imperative to squeeze more computing power from smaller devices has led to a phenomenon described by “Moore’s Law,” which observes that the number of transistors on an IC doubles about every two years. Today, even a pocket calculator has immensely more processing power than the computer that guided Apollo 11 to the moon in 1969. Pushing forward this technological frontier has required progressively greater technical know-how and larger investments, with the returns to successful firms rising in tandem. The result has been global market consolidation in the semiconductor manufacturing business: Over the past two decades, the number of companies operating leading-edge semiconductor fabrication plants has fallen from around 20 to just two, namely South Korea’s Samsung and Taiwan’s TSMC.

Similar pressures have operated on other steps of the semiconductor value chain.[1] The result is a semiconductor industry that is structured by a highly specialized division of labor between different countries, with many niches dominated by a handful of companies. Prominent examples include the TSMC-Samsung duopoly in leading-edge fabrication (manufacturing of the physical chips), and the monopoly in extreme ultraviolet lithography (EUV) systems, which are required for cutting-edge fabrication, by the Netherlands firm ASML. The complexity of the technologies involved and the incumbent advantages make these industry leaders effectively unchallengeable within their niches over the short term.

These supply chain characteristics run against the political imperative to “onshore” semiconductor production, which is being inflated by the flow-on effects of semiconductor shortages during the COVID-19 pandemic and intensifying international competition in strategic technologies. The U.S. has “weaponized” the semiconductor supply chain through export control measures targeting Huawei, SMIC, and other

Chinese firms that rely on foreign inputs to perform their core business. In response, China is redoubling its efforts to build domestic industries' capacities along all segments of the semiconductor supply chain to mitigate risk from political tensions with the U.S. and its allies (Lee and Kleinhans, 2021). The European Union, South Korea, Japan, and Taiwan are also running programs aimed at bringing a bigger chunk of the semiconductor supply chain within their borders, framed by the language of "technological sovereignty," "strategic autonomy," and supply chain security.

In addition to being a ubiquitous foundational technology, semiconductors are also a critical enabler for emerging technologies such as artificial intelligence (AI). The U.S. National Security Commission on AI in its final report of 2021 recommended restricting the export of certain semiconductor-related technologies to China in order to curb development of Chinese AI-enabled military capabilities.[2] Rising computerization of devices is making semiconductors critical to a range of economically important sectors such as the automotive industry, where the effects of semiconductor shortages have focused U.S. and European government attention on the implications of foreign dependence.

As the Internet of Things and digital data flows continue to expand exponentially, the cybersecurity risks from connections through digital networks are rising in tandem. Increasingly, the ability to cut potentially hostile actors out of the supply chain is viewed as the most effective means of mitigating the risk of espionage. For example, the location in mainland China of much of the global semiconductor supply chain's assembly, testing, and packaging (ATP) capacity raises the prospect of so-called "hardware hacks" by Chinese authorities, such as the covert insertion of additional components for intelligence collection or sabotage.[3] Onshoring the semiconductor supply chain, or at least "friendshoring" it to countries perceived as friendly, is increasingly regarded as a precondition for national cybersecurity.

Current policies. Semiconductors were one of four technologies targeted by the Biden administration's 100 Day supply chain reviews, a report for which was released in June 2021 (White House, 2021). The report's conclusions on semiconductors were that U.S. industry has many strengths along the supply chain, but also critical gaps in fabrication, manufacturing equipment (lithography), materials, and ATP capacity. The recommendations included financial support for onshoring initiatives and for the U.S. semiconductor ecosystem generally, engaging allies and partners to harmonize semiconductor-related policies and invest in the U.S., and using export controls and foreign investment reviews to protect U.S. technological advantage and address national security concerns.

The Biden administration has emphasized that the U.S. is in an international "competition to win the 21st century" through technological leadership. Furthermore, the debate over industrial policy for semiconductors is taking place in the context of a growing push for onshoring critical technology supply chains in general. For example, in 2021, Sen. Josh Hawley introduced draft legislation — the "Make in America to Sell in America Act" — that would impose local content requirements in sectors deemed by the federal government as critical to national security and protection of the U.S. strategic industrial base.[4]

The U.S. Department of Defense has long run a "trusted foundry" program for procuring microelectronics from security-vetted suppliers, but this approach has come under strain as U.S.-based companies have fallen behind in leading semiconductor fabrication. The Defense Advanced Research Projects Agency (DARPA) is funding projects and engaged in public-private partnerships aimed at developing U.S. industry in fabrication and advanced packaging.[5] DARPA also funds R&D for compound semiconductor materials — notably silicon carbide and gallium nitride— that have particular applications and may represent new frontiers for technological development.

U.S. policy measures directed at strategic competition with China in this sector are commonly typified as "run faster" or "trip the opponent." On the "run faster" side, in August 2022 the U.S. passed the CHIPS and Science Act, which provides subsidies for semiconductor R&D and construction of fabrication plants inside the U.S. These are tied to "trip the opponent" measures in the form of requirements for subsidy recipients not to engage in equivalent activities in China, with an exception made for capacity related to "legacy semiconductors."[6] This refers to older-generation processes that are limited to producing chips with lower transistor density, with the CHIPS Act reserving interpretation of the exact meaning of "legacy" to U.S. authorities.

In September and October 2022, the Biden administration doubled down on a "trip the opponent" approach with a major expansion of export controls targeting China's semiconductor industry and sectors that depend on AI and high-performance computing. The promulgation notice for the October measures justified them in terms of restricting Chinese "military modernization, including the development of weapons of mass destruction (WMD), and human rights abuses."[7]

In September, National Security Advisor Jake Sullivan framed these steps as a transition in U.S. strategic technology policy, from staying a couple of generations ahead of China to maintaining "as large of a lead as possible," "given the foundational nature of certain technologies, such as advanced logic and memory chips."[8] In early October, U.S. Trade Representative Katharine Tai reinforced this message by describing China's industrial policies as a threat to the survival of free societies including the U.S., requiring Washington to prioritize supply chain security above free trade.[9] As of mid-October 2022, the exact scope and application of the expanded controls targeting China's semiconductor sector remained unclear and subject to public consultation and adjustment by the U.S. Commerce Department, but the key points can be summarized as follows.

Most of the new rules apply to all entities in China, using a new regulatory category of "regional stability." The controls are therefore specific to China and justified by characterizing China as a threat to regional stability, rather than by the nature of the controlled items themselves. The new controls target semiconductor manufacturing equipment (SME) and certain advanced computing ICs and memory chips, focused on AI and supercomputing applications. Exporting these items and services to an entity operating in China now requires a license from the U.S. Commerce Department, application for which is generally subject to a presumption of denial.

Furthermore, non-Chinese entities are restricted from supplying Chinese customers with the controlled items where their production involves U.S.-origin technology, which is extensively present throughout the global semiconductor supply chain. Additionally, one new rule amends the criteria by which U.S. regulators can add an entity to the "entity list," which subjects the entity concerned to extended controls and licensing requirements. These criteria now include "a sustained lack of cooperation by the host government… that effectively prevents" U.S. authorities from determining compliance with export controls, in particular end-use checks.[10]

"U.S. persons" are now restricted from working in China in activities related to these controlled items unless granted a license by the U.S. Commerce Department. This will affect a significant number of individuals in China's semiconductor industry who hold U.S. citizenship and are heavily represented in the startup firms trying to plug gaps in China's domestic capabilities. This rule seems to encompass potential offshoring activity by U.S. entities, to deter them from transferring technology and know-how to non-U.S. entities that then sell to Chinese customers.

Although nominally confined to advanced semiconductors and related items, these rules amount to a technological containment strategy, reflecting an expanded concept of U.S. national security and China's identification as the primary threat in this context. In his September speech, Jake Sullivan rejected the distinction between domestic issues and national security "when facing a competitor that is determined to overtake U.S. technological leadership" and competing "to lead in the industries of the future."[11] While the new rules are justified in terms of military uses and human rights abuses, the foundational and dual-use nature of advanced ICs and high-performance computing means that these controls will hamper development of China's civilian economy on a broad front, particularly in emergent sectors like self-driving vehicles and intelligent manufacturing that Beijing has identified as priority national development goals. Furthermore, in practice many of the newly controlled technologies are not precisely related to the advanced capabilities that are nominally being targeted but have wider application. This means that supplies to Chinese customers with respect to older-generation capabilities may be seen as risking violation of the new rules, with deleterious effects for Chinese industry that are much wider than the framing of the new controls would suggest.

The new controls took effect immediately and rapidly provoked industry responses. Within days of the October rules' promulgation, one of the leading SME suppliers — a U.S. firm whose largest market is China — reportedly instructed staff that it would immediately cease offering certain supplies and services to China-based customers, including third-country companies operating in China like South Korea's SK Hynix.[12] However, the presumption of denial for license applications under these controls does not apply for companies headquartered in specified countries. This reflects consideration for South Korea and other U.S.-allied governments concerned about impacts on their economies and technological champions from being forced to terminate business in and with China in semiconductors. Several foreign industry leaders including SK Hynix and TSMC have already received one-year licenses under the new rules to continue operations in China.

A major obstacle to U.S. reshoring efforts, as acknowledged in the Biden administration's supply chain review, is that the U.S. is not a cost-effective location for many activities along the semiconductor supply chain. This has also been highlighted by TSMC's former and current leaders in statements about the company's plans for operations in the U.S.[13] The sums being debated in Congress are too small to achieve major shifts in the global supply chain over the short term, when compared against the industry's numbers. For example, TSMC is spending $44 billion on capital expenditure in 2022 alone, while Samsung's semiconductor foundry division is projected to be generating over $50 billion in annual revenue by the late 2020s, with some 70% of revenue currently being reinvested in production capacity.[14]

This makes it unlikely that any U.S. player will be competitive at scale with either TSMC or Samsung for the foreseeable future, although Intel is attempting to reestablish itself in the cutting-edge fabrication market. The U.S. government has made efforts to persuade TSMC and Samsung to locate operations in the U.S., and both have responded with significant capital investments. But both companies also appear likely to continue building cutting-edge plants in their home jurisdictions, perpetuating the risks entailed from the viewpoint of U.S. policymakers.

For China, the situation is far more challenging, even before the effects of the October 2022 export controls are factored in. Although Chinese industry has made significant progress in many steps of the semiconductor supply chain and gained notable market share in a few segments, Chinese firms are not industry leaders in any step and remain incapable of producing cutting-edge products in critical niches. It is these gaps that are being exploited by U.S. export controls that effectively impose secondary sanctions on third parties for doing business with Chinese companies, which depend on foreign (including Taiwanese) companies for critical processes such as fabricating cutting-edge chips.

Chinese authorities have been trying for decades to promote development of the domestic semiconductor industry. In 2014, the national government created a top-level bureaucratic steering committee (leading small group) and a state-linked investment fund (the so-called “Big Fund”) to drive development of China’s semiconductor sector. This represented an effort to harness the private sector’s energies toward strategic priorities set by state authorities, in line with the “top-level design” approach to policymaking under Xi Jinping’s leadership.[15]

This approach was premised on China’s participation in the transnational semiconductor supply chain. Chinese firms were able to become competitive in some capabilities while relying in other areas on foreign vendors, most notably TSMC and other foundries for leading-edge fabrication. Chinese firms were also able to build market share and technical know-how through mergers and acquisitions of foreign entities, especially in ATP, where mainland China-based companies became the second-largest bloc by market share, after Taiwanese firms.

Over the past half-decade, the Chinese government has responded to growing pressures from the U.S. to promote supply chain “decoupling” from China by doubling down on import substitution efforts. Over 2020-2021, Chinese national agencies introduced three sets of measures providing targeted support for the semiconductor sector that include tax relief, direct financing and subsidies, regulatory guidance, and skills development. Semiconductors were one of seven frontier technologies prioritized by the 14th Five-Year Plan released in March 2021. This signal of strategic importance led to a proliferation of semiconductor industry development plans by provincial and municipal governments across China.

Policy emphasis seems to be moving to advanced packaging techniques and compound semiconductor materials, being fields in which Chinese industry has some prospect of leapfrogging the gap with foreign industry leaders. Compound materials were the only reference to semiconductors in China’s 14th Five-Year Plan for National Informatization released in January 2022. They also feature prominently in policies being released by subnational governments, notably in the Shanghai government's ICT sector development plans, which include the ambition for a Silicon Carbide Valley" industrial cluster.

All these new policies emphasize developing a complete semiconductor ecosystem, relying on synergies between companies at different steps of the supply chain. Political rhetoric increasingly exhorts a "whole-of-nation" approach to reducing China's weaknesses in critical technologies, drawing on a mobilizational tradition that goes back to the strategic defense projects of the Maoist era. Chinese authorities may be developing a successor to the '02 Special Project, a decade-long program launched in 2009 that targeted priority semiconductor-related technologies for development by combined efforts from Chinese companies and research institutions. However, a new round of such specific cross-industry R&D goals has yet to be publicized.
Overall, China remains heavily reliant on foreign inputs in the semiconductor sector, reflected in the well-known statistic of the nation's semiconductor imports now exceeding the value of its oil imports. But this statistic also reflects the concentration of global electronics manufacturing in China, which has so far provided strong incentives for foreign firms to remain engaged with Chinese markets and leverage for Chinese authorities: Xi Jinping has emphasized the need to 'pull tight' global supply chains to China.

Since the new U.S. export controls of late 2022 are confined to certain categories of advanced semiconductors and items required to produce them, large sections of the Chinese semiconductor industry should be able to remain integrated with global supply chains and markets. But unless Chinese industry can quickly substitute at scale for the technologies controlled by the new U.S. rules, either by developing them domestically or by procuring them from third countries, China will lose its potential first-mover advantage in many of the emerging civilian and military applications that its semiconductor policies were intended to support.

Proposals for finding firmer ground. The policy approach represented by the CHIPS and Science Act, and especially by the expansion of U.S. export controls in September and October 2022, has for the time being removed any prospect of finding common ground between the U.S. and China on strategic policy for semiconductors. The Biden administration now appears committed to a goal of containing China's development in this sector and in strategic technologies built upon it, without clear distinction in practice between civilian and military applications. This is unlikely to change with a future return to a Republican administration. For its part, China's government has characterized the expanded controls as designed to maintain U.S. "technological hegemony" and "to hobble and suppress the development of emerging markets and developing countries."[16]

An important factor will be the willingness of third-party countries to cooperate and coordinate with U.S. measures. To date, the U.S. has had limited success in bringing allied governments and their leading companies on board with U.S. policy initiatives for the semiconductor sector. The U.S. Commerce Department's 2021 request for information from actors throughout the global semiconductor supply chain — which was accompanied by implied threats to compel cooperation from foreign companies if necessary — was poorly received in Taiwan and South Korea, where it was seen as overbearing and creating risks of proprietary information leaking to U.S. competitors. Discussions over a putative U.S.-led "Chip 4 Alliance" with Japan, South Korea, and Taiwan also did not appear to have delivered any significant outcomes as of mid-October 2022.

European ambitions for "technological sovereignty," which are clearly expressed in the EU Chips Act proposal of early 2022, are likely to impose constraints on coordination with Washington. At a press briefing in October on the new semiconductor export controls, U.S. officials conceded that they had not secured any promises that allied nations would implement similar measures and that discussions with those nations were ongoing.[17] Conversely however, the importance of the U.S. economy and the amount of U.S.-origin technology present throughout the global semiconductor industry means that in many cases, attempting to circumvent U.S. export controls to continue business with Chinese customers would be highly risky.

Furthermore, the risk of doing business with Chinese entities has been amplified beyond presently controlled items by the amendment to criteria for addition to the U.S. entity list. As one commentator summarized this change, in sectors targeted by U.S. controls, "Any company in China can be cut off from worldwide supply chains ... through the justification that China does not cooperate with the U.S. (regulators)."[18] The only way to avoid this is unreserved submission to U.S. government demands for information disclosure. It is unlikely that any Chinese firm will take such an approach, which would run counter to Chinese domestic political imperatives and data security regulation, and on account of the latter would likely violate specific Chinese laws.[19]

The sweeping new export controls targeting semiconductors and the policy framing provided by the national security advisor suggest that the U.S. government has reached a consensus that at the advanced end of these technologies, "hard decoupling" and restricting Chinese capabilities must be the priority, even if this involves significant harm to U.S. industry. Furthermore, Washington is pursuing this policy unilaterally in the acknowledged absence of cooperation by allied countries, in the hope that they can be persuaded to adopt similar measures and so effectively align against China in their future economic and technological development. Given the foundational nature of semiconductors, the new U.S. controls create the conditions for a true bifurcation in global technology ecosystems. It remains to be seen whether third parties will find these new conditions sufficient reason to reverse the progress of economic integration with China that for many countries has been a consistent trend for the past quarter century.[20]

Notes:

[1] Jan-Peter Kleinhans. 2020. ‘The Global Semiconductor Value Chain: A Technology Primer for Policy Makers.’ Stiftung Neue Verantwortung. https://www.stiftung-nv.de/de/publikation/global-semiconductor-value-chain-technology-primer-policy-makers

[2] National Security Commission on Artificial Intelligence. 2021. Final Report, National Security Commission on Artificial Intelligence, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

[3] John Lee and Jan-Peter Kleinhans. 2021a. ‘Mapping China’s semiconductor ecosystem in global context: Strategic dimensions and conclusions.’ Mercator Institute for China Studies and Stiftung Neue Verantwortung. https://merics.org/en/report/mapping-chinas-semiconductor-ecosystem-global-context-strategic-dimensions-and-conclusions

[4] Josh Hawley. 2021. ‘The Only Way to Solve our Supply Chain Crisis is to Rethink Trade’. New York Times. https://www.nytimes.com/2021/10/29/opinion/hawley-supply-chain-trade-policy.html

[5] Defense Advanced Research Projects Agency. 2021. ‘DARPA Joins Public-Private Partnership to Address Challenges Facing Microelectronics Advancement’. https://www.darpa.mil/news-events/2021-12-22

[6] Paul Triolo. 2022. 'U.S. finally passes semiconductor subsidy bill, but it’s not going to help competition with China'. The China Project. https://thechinaproject.com/2022/08/18/u-s-finally-passes-semiconductor-subsidy-bill-but-its-not-going-to-help-competition-with-china/

[7] See 2022-21658.pdf (federalregister.gov). Bureau of Industry and Security 15 CFR Parts 734, 736, 740, 742, 744, 762, 772, and 774, Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification.

[8] See Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit. The White House. https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/

[9] See Remarks by Ambassador Katherine Tai at the Roosevelt Institute's Progressive Industrial Policy Conference. Office of the United States Trade Representative. https://ustr.gov/about-us/policy-offices/press-office/speeches-and-remarks/2022/october/remarks-ambassador-katherine-tai-roosevelt-institutes-progressive-industrial-policy-conference

[10] See Department of Commerce Bureau of Industry and Security 15 CFR Part 744 'Revisions to the Unverified List; Clarifications to Activities and Criteria that May Lead to Additions to the Entity List'. https://public-inspection.federalregister.gov/2022-21714.pdf

[11] See Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit. The White House. https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/

[12] Josh Horwitz. 2022. 'Exclusive: KLA to stop sales and service to China to comply with U.S. export curbs'. Reuters. https://www.reuters.com/world/china/exclusive-kla-stop-sales-service-china-comply-with-us-export-curbs-source-2022-10-11/

13] Charlie Campbell. 2021. ‘Inside the Taiwan Firm That Makes the World’s Tech Run.’ TIME. https://time.com/6102879/semiconductor-chip-shortage-tsmc/

[14] Bogdan Solca. 2022. ‘Samsung plans to overtake TSMC by 2030.’ NotebookCheck. https://www.notebookcheck.net/Samsung-plans-to-overtake-TSMC-by-2030.593861.0.html

[15] John Lee and Jan-Peter Kleinhans. 2022. ‘Europe’s dependence on Chinese semiconductor manufacturing’. In Digital Power China Research Consortium. ‘China’s Digital Power: Assessing the Implications for the EU’. https://timruhlig.eu/ctf/assets/x93kiko5rt7l/4uiZoNQtRkni5KfuNDrBbx/fd52e3320cfe21e6b304ad31d81279d8/DPC-full_report-FINAL.pdf

[16] Mark Magnier. 2022. 'Tech war: Washington takes new steps to frustrate China, advance US chip-making | South China Morning Post'. South China Morning Post. https://www.scmp.com/news/china/diplomacy/article/3195254/tech-war-washington-takes-new-steps-frustrate-china-advance-us

[17] Stephen Nellis et al. 2022. 'China and USA Are Officially At Economic War – Technology Restriction Overview – SemiAnalysis'. Reuters. https://www.reuters.com/technology/us-aims-hobble-chinas-chip-industry-with-sweeping-new-export-rules-2022-10-07/

[18] Dylan Patel. 2022. 'China and USA Are Officially At Economic War – Technology Restriction Overview'. Semianalysis. https://www.semianalysis.com/p/china-and-usa-are-officially-at-economic

[19] John Lee. 2022. 'Cyberspace Governance in China: Evolution, Features and Future Trends'. Institut français des relations internationales. https://www.ifri.org/en/publications/notes-de-lifri/asie-visions/cyberspace-governance-china-evolution-features-and-future

[20] John Lee. 2021. ‘The Internet of Things: China’s Rise and Australia’s Choices’. Lowy Institute. https://www.lowyinstitute.org/the-interpreter/china-australia-internet-things

VIII. Opportunities for Dialogue

Challenges and opportunities. As the sections above have outlined, economic, political, and social factors shape the space for U.S.-China dialogue on the future of technology. Technology is a suite of tools embedded in economic activity, law enforcement, defense modernization, and social space. The ways a government regulates and promotes technological development is unique to its political and market system — and between the U.S. and China, these systems' differences contribute to mutual strategic mistrust.
Each side has different preferences for the role of the state in the market. The U.S. has moved over several decades to deregulate most industries on the premise that market decisions are more efficient and profitable than state intervention. China has cycled through periods of loosening and tightening state control of the market to balance the benefits of market freedom against the political and economic risks of wealth and power bubbles in an authoritarian one-party system. When the U.S. argues that China is creating an unfair playing field for normal economic competition, it is often due to policies that China sees as necessary for its long-term political economy. A frank and authoritative dialogue on each side's drivers of tech policy decision-making would help contextualize policy developments and test assumptions about each side's ultimate goals; however, system differences also distort the opportunities for a productive dialogue.

Each side has different standard operating procedures for bilateral dialogue and diplomacy. The U.S. changes personnel and priorities with incoming administrations and typically allows working-level officials wide latitude to negotiate within the political mandate (i.e., to explore what is possible). Chinese officials tend to stay long-term in one issue area but often have very little room to suggest policy changes without explicit top-down direction. These differences have led to negotiation fatigue between the two sides, particularly in the absence of a wide-ranging diplomatic process that filled these gaps.

Both sides have perceptions of the risk environment that increase bilateral friction. Put simply, Chinese technology is seen in the U.S. as an extension of party-state assets and technological cooperation as aiding a competitor or rival. As China trends toward tighter party-state control of the private sector, the U.S. evaluates new Chinese regulations on their potential to create strategic vulnerabilities and new U.S. regulations on their potential to defend against these vulnerabilities. Meanwhile, China views the U.S. emphasis on personal freedom and electoral democracy as a strategic risk in adopting U.S. technology and social platforms.

A roadmap to a productive bilateral dialogue between the U.S. and China on emerging technology must manage the following challenges:

1. Keeping expectations realistic. Technology's dual-use applications and pervasiveness in everyday life has exponentially widened the national security community's perception of risk in U.S.-China cooperation. The amount of dialogue necessary to let technology discussions drive better bilateral understanding and cooperation is unlikely to materialize. Instead, fewer dialogues should prioritize high-level management of the key priority issues: the role of AI in warfare, IoT standardization, ethics and norms in data collection, and fair use of cyber tools.

The output of these dialogues might be limited to reducing misperception by investigating the other side's evolving position on these topics. However, regularized dialogue may identify sufficient common interests — for example, requiring human confirmation of AI decision-making in warfare — that can lead to formal negotiations and agreements. IoT standardization discussions can address concerns about backdoor capabilities built into objects by SOEs and national champions.

Keeping expectations to issue management may forestall use of the dialogues themselves as leverage, as when the U.S.-China Cyber Working Group (CWG) was cut off by Beijing in the aftermath of the U.S. indictment of five Chinese military officers on cybertheft charges. Though a high-level dialogue was reinstated through a 2015 Xi-Obama summit joint statement, this dialogue was only held once more after being renamed in the Trump administration. Reaffirming the five principles reached in the Obama-Xi agreement again in the Biden administration would be a stabilizing factor in bilateral relations and proof that U.S. agreements can be sustained throughout swings in domestic politics.

U.S.-China military-to-military dialogues provide a useful analogy and point of optimism. After China cut off military-to-military dialogues many times over U.S. arms sales to Taiwan, these dialogues had become useful and necessary mechanisms that survived the breakdown of other diplomatic dialogues after the 2017 U.S. National Security Strategy emphasized great power competition as a guiding principle of U.S. strategy toward China. Issue management, therefore, seems to be an area where dialogue is both possible and stabilizing.

A focus on issue management does not preclude agreements on underlying principles in new areas. While more generalized and likely less enforceable than desired, coming to bilateral agreement on basic principles can be seen as a component of issue management and serve to deepen understanding on how the two sides see the major issues from their own political and historical context. The point would not be to change the other side's view, but to see at what level the two sides' interests overlap, no matter how general.

2. Getting the right people together. Because the use of technology cuts across social, economic, and military paradigms, many different government agencies participate in the policymaking process. For example, the charter of the U.S. National Science and Technology Council Select Committee on Artificial Intelligence mandates membership from 10 different government agencies or sub-agencies.[1] In China, tech policy often overlaps among a similar number of agencies, including some that have no direct corollary in the U.S. system. To compare on AI rules-making, China has three bodies— the Cyberspace Administration of China, China Academy of Information and Communications Technology, Ministry of Science and Technology — contributing frameworks and rules to an overall governance regime.[2]

A first step in initiating a productive issue-management dialogue between the U.S. and China is to identify the correct interlocutor on the technology issue in question. With whom should the Ministry of Science and Technology personnel communicate in the U.S. system, which has no equivalent Cabinet department? Previous large-scale engagement efforts, such as the U.S.-China Strategic and Economic Dialogue, successfully navigated these various divisions of labor and responsibility by establishing robust working-level relationships. A similar process would need to develop to put the right people together on technology policy issues.

U.S. officials may also need to seek input from or incorporate feedback from private-sector actors into the dialogue. In the current political climate, joint research seems out of the question. However, the moving target of technological innovation and the specific issues that could be remedied through dialogue and consultation — supply-chain bottlenecks, cybersecurity concerns, and so on — requires the private sector to periodically weigh in. China closes this knowledge gap through several formal mechanisms that reduce the space between state and industry; the U.S. needs to make sure that its structure of government-industry knowledge-sharing is likewise robust.

3. Setting the agenda. Both countries are seeking a competitive edge over the other and will not want to share specifics on their progress, particularly as new technologies and tools are developed. A workable agenda for U.S.-China tech dialogue would cover the broadest and the narrowest issues and leave the space between off-limits; for example, the two sides can discuss rules for fair use of cyber tools in peacetime (broad), or resolve specific customs issues (narrow), but are unlikely to seek renewed research collaboration on sensitive technologies.

One component of bilateral dialogue and exchange on technology issues must be each side’s interpretation of rules of fair use of cyber tools. With the dual-use capabilities described in the sections above, the U.S. and China are likely to have some degree of mutual vulnerability to cyberattacks, potentially ones that target big data sets, use AI capabilities and/or occur over 5G networks. A sound deterrence strategy requires each side to know exactly what is escalatory or unacceptable to the other side. By defining these parameters, both sides can then be clear on what practices are perceived as outside the bounds of fair use and therefore risk retaliation.

Relatedly, the two sides can continue to discuss their different approaches to data storage and privacy, though neither side should expect to change the fundamental position of the other on these issues. Through discussion, both sides should recognize that their differences lie in their respective justice systems and not in the tools themselves.

Supply-chain issues, particularly those related to semiconductors, will not be a productive area for bilateral dialogue, but discussions on macroeconomic stability are of common interest and could touch on the disruptions associated with bifurcating the technology supply chain as well as any accusations of weaponized interdependence regarding the necessary minerals and elements in technological production.

4. Committing to a regular schedule. Regularization of a dialogue can mitigate certain challenges. First, the rapid pace of innovation requires constant agenda adjustments on which one or both sides may be reluctant to agree. Regular meetings can help each side understand one another’s views and trajectory, and work through potential conflict regarding misperceptions of technology policies.

Second, a regular schedule creates an action-forcing mechanism for both systems to conduct internal reviews and formalize policy. Since each side will be required to discuss technology-related issues with one another, internal plans must be consistent with dialogue talking points, requiring each state to understand the positions of its different stakeholders and ensure policy guidance is in place.

Third, a regular schedule builds relationships. This is particularly important because U.S. officials can change from administration to administration. Regular meetings can allow both sides to assess the personalities and interests of individual participants and to strengthen ties among them. Because of the differences in bureaucratic responsibilities outlined above, these relationships may also prove useful on issues not covered in the technology dialogues.

Finally, a regular schedule allows a long-term approach to bilateral discussion on technology issues. Many of these issues cannot be resolved or shelved. Knowing that another meeting is already on the calendar reduces pressure to prematurely declare the failure of dialogue and diplomacy; as a result, gains can snowball over time.

5. Managing the interplay between bilateral discussions and international institutions and agreements. The U.S. and China each have considerable weight in the international system. Where bilateral agreements are in place — such as the Obama-Xi principles for cybersecurity — the two countries could push for expanded adoption of such principles in larger multilateral formats. In other words, the bilateral agenda should be the starting point for establishing global rules and norms. Bringing the rest of the world on board with relatively benign principles, such as timely responses to official inquiries on cyber activity or that no government actors should participate in the theft of intellectual property, would reinforce major power accountability to these tenets.

A discussion on rules can not only stabilize the bilateral relationship by putting guardrails on the use of technology, but also pave the road for forward-leaning discussions with other major powers and global actors. Both the U.S. and China are sufficiently powerful to ignore rules imposed by one side on the other; the only enforceable rules-based order on technology tools will be reached via dialogue and negotiation.

Where agreements — even on basic principles — are often impossible, multilateral mechanisms can expand and supplement the conversation. Outside of U.S.-China strategic competition, rules and regulations in the EU areas are driving standards and norms on data privacy. And, as suggested above, a global governance framework or institution that can address cyberconflict should consider the U.S. and Chinese positions on technology rules and norms. However, any such framework must consider the very high start-up costs —including time, political buy-in, and money — associated with creating a new institution as well as the fact that current institutions face significant obstacles given heightened major power competition. Any institution will find it incredibly difficult to function in the absence of bilateral agreements or multilateral agreements that include both Washington and Beijing. Already, the dominant trend is toward using international institutions as an arena of major power competition rather than as a venue for consolidating common interests. Perhaps this may have to be an area for tentative, early exploration.

Notes:

[1] Trump White House. 2018. Charter of the U.S. National Science and Technology Council Select Committee on Artificial Intelligence, 2018) Trump White House Archives, Jan 5, https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/Charter-Select-Committee-on-AI-Jan-2021-posted.pdf

[2] Matt Sheehan, 2022, China’s New AI Governance Initiatives Shouldn’t Be Ignored. Carnegie Endowment Commentary, January 4, https://carnegieendowment.org/2022/01/04/china-s-new-ai-governance-initiatives-shouldn-t-be-ignored-pub-86127

IV. Conclusion

Greater transparency, discussion, and cooperation are critical components of reducing the risk of technology conflict. Even though the U.S. and China must treat technologies as areas of high national security interest, both countries should recognize that the new technology landscape does not need to derail their common concerns. Technology is a suite of tools that compound underlying dynamics, integrated into economic competition, defense planning, and political values while having potentially profound consequences for society. Some of the effects of new technology — both direct and indirect — are not yet fully fleshed out, much less understood. However, these tools are not separate from existing U.S.-China dynamics but evolve in the context of political, economic, and security policy decisions.

Restoring stability in U.S.-China relations will require long-term and enduring management of emerging technology concerns. The U.S. and China should approach each other on these issues with cool heads and well-defined bottom lines. The purpose of technology dialogue is to explore where political and economic interests on technology trade and cooperation overlap, and where such interests are intractable. Technology dialogue will be most productive if it bridges gaps between the U.S. and Chinese bureaucracies and if the officials involved avoid invective while arguing for their own policies. It will be least productive if either side approaches with the goal of airing grievances about the other side's political system and economic interests.

The U.S.-China relationship was strong for many years until recent events prompted a reframing of the relationship from cooperative to competitive and confrontational. The cooperative aspects of the relationship can be rebuilt if both sides are willing to enter into good-faith dialogue, even if a political climate that allows for such exchanges to gain traction takes time to develop. The consequences of avoiding such dialogue could include prolonged global economic inflation due to decoupling and threat perceptions that could escalate regional and global instability. In the current international environment, there is little appetite for either. The U.S. and China should avoid costly mistakes that could result from refusing to talk about technology interests. Regardless of the trajectory of U.S.-China relations, holding out the possibilities for interaction and even potential cooperation remains an important aspect of the relationship.

THE
CARTER CENTER

About the Publisher

This report is published by the Carter Center's China Focus. Its editors are Yawei Liu, senior advisor on China at The Carter Center, and Michael Cerny, program associate for the Center's peace programs.

President Carter's decision to normalize diplomatic relations between the United States and the People's Republic of China in 1979 changed both countries and the world. Facilitating expanded bilateral trade, investment, and people-to-people exchange between the two countries has allowed East Asia to enjoy relative peace and prosperity for decades.

However, the U.S.-China relationship is now under immense strain. Since 2009, the Chinese Communist Party has strayed from the path of "reform and opening" that encouraged slow and steady progress toward political and economic liberalization. Washington began to criticize China's attempts to revise the international system, and Beijing responded by accusing the U.S. of containing China's rise. As President Carter wrote in February 2021, "Government officials in both countries have adopted rhetoric and policies that reflect the hostility that Vice Premier Deng and I sought to calm in 1978."

The Carter Center remains committed to preserving the legacy of President Carter and Deng Xiaoping's historic decision while adapting to the demands of the 21st century. This requires navigating a bilateral relationship fraught with global crises, ideological divergence, human rights crises, nationalist tension, and the looming threat of conflict in the Taiwan Strait. Through its research, workshops, and online engagement initiatives, the China Focus fosters greater dialogue, exchange, and critical reflection on the past, present, and future of U.S.-China relations.

Contact: In Atlanta, Maria Cartaya, maria.cartaya@cartercenter.org