Chapter 5

Recursive Exploitation

The Feedback Loop of Espionage and Innovation in China's 5G, AI, and Quantum Technology

By Richard B. Andres

This chapter explores the rapidly evolving dynamics of Great Power competition in cyberspace, including 5G telecommunications infrastructure, artificial intelligence (AI) and big data, and quantum computing. It updates and extends the analysis found in chapter 6 of Strategic Assessment 2020: Into a New Era of Great Power Competition, *which is anchored in the observation that the United States and China intensified their overt competition for future dominance in AI, massive data collection, and the control of cybercommunication on land, at sea, in the air, and in outer space.*[1]

The past half-decade featured an explosive entrance of AI into public consciousness and popular conversation. China is currently investing seriously in three critical new information technologies—5G wireless, AI, and quantum computing—that, as part of its information strategy, could vastly increase China's control of the global flow of information. The United States has a short window to contest China's state-led ascent in these technologies and in the underlying conditions that are allowing China to outpace the United States in this wider field. Although the United States has made some progress in the period from 2021 to 2024 against China, if the Nation does not prevent China from dominating global flows of information, China could attain a clear advantage in its rise to replace the United States as the world's leading Great Power by 2030.

For much of the last century, America's technological superiority has been one of the principal pillars by which it maintains the free world order in the face of Great Power competitors with different preferences for the international system. Traditionally, by maintaining a clear edge in innovation, the United States has offset the demographic and industrial advantages of competitors like the Soviet Union and, more recently, the People's Republic of China (PRC). However, this technological foundation now faces an unprecedented challenge. Over the past two decades, the PRC has closed the gap in critical

technologies.[2] A recent assessment by the Australian Strategic Policy Institute (ASPI) finds that China currently leads global research in 57 of 64 critical technologies, while the United States maintains leadership in only 7.[3]

This chapter explores the current technological competition between the United States and China from a geopolitical perspective, tracing its origins to the 1990s. During this period, the United States leveraged its leadership in digital information technology (IT) to implement a global strategy focused on breaking down barriers to information, with an aim of liberalizing autocratic states like China. In response to this potentially existential threat to its authority, the Chinese Communist Party (CCP) began to use a combination of centralized planning and focused economic espionage to offset and eventually overcome the U.S. lead in IT. As implemented, the PRC's approach was recursive, with advances in IT facilitating greater success at economic espionage, which further improved its advances in IT. Currently, this contest focuses on three technologies: 5G wireless networking, AI, and quantum computing. Perhaps ironically, according to the ASPI longitudinal study these are among the only technologies in which the United States still holds small advantages over China.[4]

While the United States traditionally acted as if China were not a competitor and no advanced technology race existed, Chinese geopolitical theorists have long asserted that the Great Power that wins the race to dominate IT will have unprecedented capability to use its advantage to win geopolitical advantage and that IT is key to determining the character of the future world order.[5] Chinese President Xi Jinping has regularly and emphatically repeated these themes.[6] Viewed through this lens, the three technologies described herein are at least as important to the outcome of the current Great Power contest between the United States and China as the conventional arms races currently unfolding in the South China Sea. Although the generous vision the United States developed for dealing with information in the 1990s was highly effective at one time, it is no longer suitable given China's approach to information conflict. Addressing the growing technology gap between the United States and China will require rethinking on how the United States treats both IT and information itself. To stand a chance in the technology race with China, the United States must recognize IT as a cornerstone of Great Power competition and work to establish a digitally bordered world that excludes malicious Chinese actors.

This chapter is organized into three sections. The first examines the historical and strategic origins of the U.S.-China technological rivalry. The second assesses China's approach to 5G, AI, and quantum computing technologies. The final section outlines a strategic roadmap for U.S. policymakers to counter China's ambitions and strengthen the liberal international order.

The Geopolitical Foundations of the U.S.-China Technological Rivalry

To understand what is happening in the current technological competition between the United States and China, it is necessary to understand the historical roots of the rivalry and how the conflicting U.S. and Chinese geopolitical information strategies led the two superpowers to the current situation. It is also important to understand the divergent U.S. and Chinese perspectives. Until relatively recently, the United States has downplayed the competition while for the last three decades China has viewed the contest in existential terms.[7]

In the years following the Cold War, the United States initially maintained a perspective rooted in Great Power politics. By the late 1990s, however, it had largely embraced the belief that democracy had achieved a permanent victory and that the era of geopolitical competition between Great Powers had come to an end. As a result, it refocused its geopolitical goals away from Great Power competition and toward remaking the world by focusing its foreign economic policy on what political scientists term *absolute* rather than *relative* gains and its foreign security policy on human rights and democratization. Actions designed to foster democracy were often made with the consent of the countries in which the United States acted, but in several dozen cases, including China, its efforts were strongly opposed by the ruling regimes in the nations it attempted to influence.

A cornerstone of America's strategy for global liberalization was its digital information freedom policy. This approach aimed to leverage digital networks to foster global prosperity by sharing technology and opening markets, with the expectation that autocratic beneficiaries would, in turn, adopt more democratic practices.[8] Central to this effort was the creation of an open global Internet and a consistent tolerance for commercial espionage and intellectual property theft by developing nations, particularly China. The policy also involved the deliberate sharing of scientific and technological advancements, driven by a charitable desire to stimulate economic growth in developing countries, including China.[9] Additionally, global businesses played a role by spreading technology through market incentives. At its core, this strategy was underpinned by a Cold War–era geostrategic worldview that regarded the dissemination of technology as inherently beneficial to the world after the fall of the Berlin Wall as it had been for the post–World War II Western partners before the wall fell.

While historically uncommon for Great Power hegemons, the strategy of sharing wealth and technology with geopolitical rivals was not without precedent. During the Cold War, the free flow of information played a crucial role in the West's victory. The Soviet Union's inability to prevent its citizens from getting information about the advantages of free markets and democracy contributed to its collapse. The United States also leveraged economic aid and technological diffusion to stabilize developing nations and shield them from communist influence—the idea being that access to information and particularly technology improved nations' prosperity, which in turn led to political stability and liberalization.

Given this history, the post–Cold War expectation that economic integration and digital openness might liberalize authoritarian regimes like China was not entirely unfounded. From the Marshall Plan onward, the United States effectively used market-driven development to counter autocracy, making it logical for policymakers to extend this approach into the digital age.[10] Initially, these strategies appeared successful: technology transfers and global digital connectivity likely contributed more to poverty reduction than any prior force in history.[11] Moreover, for at least two decades, the open Internet facilitated uprisings against authoritarian regimes, exemplified by the Color Revolutions in Europe and the Arab Spring of 2011.

The central problem with the U.S. approach to freedom of digital information is that from the perspective of the CCP, it represented an existential threat. If China's people were to accept democracy and oppose authoritarianism, it would almost certainly mean the end of CCP rule. Given China's record of civil wars, such a change was likely to be accompanied by national fragmentation and bloodshed. This meant that to China's leadership, Ameri-

ca's cyber policy represented an existential threat to members of the CCP and possibly to China's population. Under these circumstances, leadership could not agree with the American idea that history had ended and that Great Power competition was over. From the CCP's perspective, failing to push back against the U.S. information policy could be fatal. To obtain the CCP objective of domestic social control and economic prosperity, the best countermove was to become powerful and purposive enough to thwart the U.S. goal.

When the Soviet Union dissolved in 1991, the CCP laid the blame largely on the interaction of the American and Soviet information policies. In the first place, the centrally planned Soviet economy had not been able to innovate technologically as fast as the West's. This allowed the democratic world's economic strength to advance much faster than the Soviet Union's. In the second, the Soviet method of trying to overcome its shortcomings, Mikhail Gorbachev's *glasnost*, which involved reducing censorship and opening to the West, had allowed what China's communists viewed as Western psychological operations to undermine and eventually destroy the communist ideological superstructure that held the Soviet Union together. The result for China's role model was catastrophic. When the Soviet Union disintegrated, its economy collapsed and its streets fell into near-anarchy, largely controlled for the next decade by organized crime and oligarchs.[12] Thus, CCP leaders surmised that, to the extent that the U.S. post–Cold War information strategy was successful, China would fall into the same trap. However, the situation would be far worse for China, as most of the many revolutions China experienced over the past two centuries ended with millions—or even tens of millions—of deaths, often involving the eradication of the members of the *ancien régime* and their families.

Throughout the 1990s, CCP strategists dedicated a good deal of effort to theorizing about the digital-age problem of how to deal with the need to open to Western technology while avoiding exposure to Western subversive democratic ideas. Much of this debate revolved around digital technologies and how to use the emerging global Internet as a tool in what was often perceived as an existential battle between China and the United States.[13]

A digital world initially put the CCP on the horns of a dilemma. China needed to exploit U.S. digital openness to develop a means of obtaining Western technology to avoid the economic catastrophe the Soviet Union experienced, but it had to do so without opening itself up to the information and democratic reforms that had caused the Soviet Union to collapse.

The central practical problem the CCP faced was how to allocate the weight of its efforts between procuring Western technology and denying Western ideology. If the CCP swung too far toward Internet censorship, it risked failing economically as its technology fell further behind the West, potentially leading to its population losing faith in communism's ability to deliver material goods. If it swung too far away from Internet censorship, it risked its subjects becoming enamored with Western ideals associated with democracy and human rights.

Theoretically, this problem could be solved by creating technological and legal systems that would allow the CCP to selectively determine what types of information could enter China from the West. Economic and technological information that would benefit the CCP should be allowed into the country and shared among actors within the country. Ideological

and political information would be censored at the border and stopped from being shared among potential dissidents within the country.

There were, however, two problems with this approach. The first was technical. Because the United States had developed the technology behind the Internet and then built the Internet's physical infrastructure, it had created its technical and normative standards and protocols. This first-mover advantage gave the United States an enormous advantage in determining what information would flow in, out, and within China. The U.S. insistence on preventing the CCP from blocking Western social and political information-sharing into and within China was a serious technological problem.

The second part of the problem was political. China's future depended on the U.S. assumption that Great Power competition was a thing of the past and that sharing technology with communist China would not pose a significant threat to the West. If China took actions that persuaded U.S. leaders that it was a threat, so long as the United States dominated the global Internet, it could reduce the flow of technology-related information to China.

To deal with these two problems, China executed a three-part strategy. The first involved using digitally enabled economic espionage to the maximum extent possible to bring Western technology to China and then use it to build domestic technology champions.[14] The second used a combination of technical and repressive measures to prevent the Chinese population from following the examples of the Soviet Union and many other countries in overturning their autocratic governments.[15] The final part involved a global information campaign aimed at allaying other nations' fears that China, and the CCP in particular, represented a threat to the U.S.-led liberal international order.[16]

The first part of China's approach to overcoming its technological deficit involved a whole-of-nation technology piracy campaign. The CCP had strongly emphasized technology transfer since its earliest days. In the 1950s, it worked closely with the Soviet Union to transfer technology. Throughout the Cold War, it employed immense efforts to transfer Western technology to China.[17] During this period, it developed both a significant technology espionage program and a series of domestic institutions—state-owned enterprises, research institutes, universities, technology parks, laws, and courts—all explicitly created for receiving and digesting foreign technology.[18]

In the 20th century, China carried out its economic espionage program enthusiastically. The program ran into enormous difficulties because of problems common to espionage:

- acquiring technology from abroad required a significant human element
- moving intellectual property (IP) pirates to foreign countries
- developing relations with foreign governments and corporate entities that would enable spies to access IP
- bringing back thousands or millions of pages of technical information.

While this program was effective at slowly moving the technology used by China's economy and military forward, it could not come close to keeping up with the rate at which technology was developing in nonsocialist nations.[19]

In the late 1990s, however, China's growing connection to the global Internet provided a potential solution to these problems. The CCP could theoretically leverage digital con-

nectivity to pirate technology at a scale thousands of times greater than would be possible through traditional nondigital methods. At that time, the lack of U.S. cyber defense protocols made IP piracy relatively easy. The main problem for China was that it did not have enough military hackers to fully exploit the lucrative targets offered by U.S. businesses and government institutions. Its solution was to outsource the mission to hundreds of thousands of freelance hackers under the guise of its cyber militia program.[20] This freelance system approach to spying was enormously effective in conjunction with its state espionage institutions. In 2009, President Barack Obama declared that these programs were stealing a trillion dollars' worth of IP each year.[21] This estimate was most likely an exaggeration of the actual cost to the United States, but it was accurate regarding its positive effect on China's economic and military development, both of which benefited greatly from the program.

As the CCP was implementing its IP piracy program, China implemented and continuously improved what became colloquially known as the Great Firewall of China to solve its potential problem with revolutionary ideas moving into China from the West. The goal of this program was to use a combination of technical and repressive methods to prevent democratic ideals from leaking into China through cyber means and to prevent CCP subjects from using digital means to conspire against the Party.[22]

To address the third leg of China's strategy, the CCP began a massive global information campaign aimed at stamping out negative speech related to China and its programs anywhere they occurred, attempting to replicate its domestic censorship policies abroad. This global information campaign employed a variety of approaches, but much of its success came down to technology. In the early era, before China developed more sophisticated methods, it resorted to hiring hundreds of thousands of so-called 50-centers, whose job was to monitor foreign chat sites and comment with the CCP's Party line.[23] When combined with regular and dire economic and sometimes physical threats to individuals and organizations around the world that challenged the CCP narrative on issues such as IP theft, the program was relatively successful. Generally, America's free speech–centric democracy did not have a way to counter China's use of a combination of digital technology and extortion to prevent citizens of other countries from publicly speaking about China's program of digital piracy.

Throughout the 2010s, the United States wrestled with how to deal with China's response to its geopolitical approach to IT. In the early years, the Obama administration regularly criticized China's digital IP theft. By 2016, faced with China's extensive and growing IP theft program, even Great Power–"end of history" optimists could no longer ignore the problem. When China's digital technology theft program began, China had a gross domestic product of around one-tenth that of the United States. By the 2010s, it was over half its size, something the Soviet economy had not achieved even at its zenith during the Cold War. Ignoring IP piracy from a weak, quiescent developing nation is one thing; ignoring it from an increasingly bellicose Great Power is something else.

In response, the Obama administration implemented several diplomatic and technical measures to counter China's technology theft program. This included taking steps to protect U.S. military institutions from Chinese hackers and diplomatic steps to deter China from continuing its current policies. At the same time, U.S. businesses, which were the main targets of Chinese hackers, took measures to protect their networks from exploitation.[24] In the

mid-2010s, in response to U.S. Government and corporate actions and because of massive improvements in its domestic digital technology capabilities, China radically changed the method it used to implement its global information strategy.

Starting around 2015, China began a rapid shift from its use of cyber militias and privateers to the sort of technically sophisticated hacking methods that had long characterized those used by countries like the United States and Russia. One of the main methods used in this new approach involved extraordinarily sizable state investments in IT. These investments focused mainly on new 5G, AI, and quantum technologies. The idea behind this approach appears to involve replicating what the United States had achieved in the 1990s as the digital technology leader. If the United States could use its technological lead to dominate cyberspace and thereby set the rules for global information flows during the first three decades of the digital age, perhaps the CCP could achieve the same thing in the fourth decade and beyond. However, doing so would require overtaking the United States as the technology leader in IT.[25]

China's Recursive Strategy for Technological Advantages

Since the mid-2010s, China has strategically allocated substantial resources toward developing technologies aimed at gaining access to and control over global digital information. The strategic shift marked a significant departure from its earlier tactics in the 2000s, which predominantly involved deploying extensive networks of hackers to illicitly acquire foreign technological advancements, positioning China as a fast follower in the global tech arena. In contrast, China's current recursive strategy leverages massive state investments in IT, which are then used for espionage to advance further advantages in IT, which are used for even more effective espionage. The current strategy aims at and is on track to produce high-tech dominance rather than parity.[26]

The primary objective of gaining technological dominance in these concentrated IT investments involves securing long-term supremacy over global information flows. Although these investments entail considerable economic inefficiencies in the short term, they are viewed in Beijing as strategically critical for achieving long-term geopolitical and economic leverage.

International 5G Wireless Infrastructure

China's foray into digital communications technology began with its 1986 5-Year Plan, which set the goal of developing a domestic industry for manufacturing telecommunications equipment. Its main action toward this goal involved a significant investment, perhaps as much as $75 billion, in a new Chinese company called Huawei.[27] Part of the CCP's push for developing a homegrown industry was the fear, years later validated by leaker Edward Snowden, that the United States had penetrated the Western equipment used by China and could employ that access to surveil Chinese users.[28]

In the early 2000s, as part of a broader PRC strategy to enhance its own telecom capabilities, the Chinese People's Liberation Army (PLA) launched a significant cyber operation against Nortel, a Canadian telecom firm and world leader in telecom equipment design and manufacturing. This decade-long hacking campaign was instrumental in elevating Huawei from a relatively obscure entity to a dominant force in the global telecom-equipment market.[29]

The operation commenced with PLA hackers infiltrating Nortel's systems to exfiltrate vital technological data and intellectual property, which was then illicitly transferred to Huawei. This transfer significantly reduced Huawei's research and development expenditures, as the company could now replicate and innovate based on Nortel's previously funded research. Consequently, Huawei was able to manufacture and market its products at a considerably lower cost than Nortel, thereby gaining a substantial competitive edge.

Furthermore, the PLA's access to Nortel's confidential communications allowed Huawei to anticipate and undercut Nortel's bids on key contracts. By consistently underbidding Nortel, Huawei not only won important contracts but also strategically eroded Nortel's market share and financial stability.

As Nortel's fortunes declined, Huawei strategically hired away its top scientists and engineers, further debilitating Nortel and bolstering Huawei's technological capabilities. This series of attacks culminated in Nortel's bankruptcy and eventual exit from the market, leaving a vacuum that Huawei was well-positioned to fill, thus establishing a strong presence in the global telecom landscape.[30]

Throughout the 2010s, China's subsidies for Huawei grew. In 2016, Huawei implemented a new standard for encoding 5G communications called Polar Code. Given massive government investments, the Polar Code marked a watershed in that it was either on par with or superior to the previously dominant low-density parity check codes then used by Western companies, elevating China to a peer competitor rather than a fast copier in telecom technology.

The CCP's support for Huawei extended beyond financial investment and espionage support. Following Huawei's development of the Polar Code, the CCP initiated a strategic campaign to promote this technology as a global standard, which compelled competing 5G providers to retool technologically. This included adopting and adapting patents and undertaking other expensive measures that enhanced Huawei's market position and augmented China's influence over global telecom standards. This campaign involved advocating for the Polar Code within international standard-setting bodies, using diplomatic and economic influence, fostering the standard in forums led by China, and advancing domestic regulations and policies that favored it.

As Huawei swept to ascendency as the global leader in 5G telecom equipment in the 2010s, the CCP took the next step in its effort to exploit its lead in information technology by subsidizing Huawei to sell equipment at rates substantially lower than those of its competitors, sometimes practically giving its equipment away. The result was that most countries around the world installed Huawei equipment in sensitive telecom facilities that had the potential to provide China with a significant ability to eavesdrop on or otherwise control the flow of information throughout the world's digital networks.

Throughout the 2010s, U.S. intelligence organizations regularly warned that China was using Huawei's equipment to spy on its customers. The temptation to buy cheap equipment, however, was irresistible for most companies and countries, and throughout the decade, even many U.S. telecom companies purchased the technology. In 2012, Huawei became the world's largest telecom manufacturer and, in 2020, the largest smartphone provider.

Starting in 2017, the United States began to limit Huawei's telecom equipment because of cyber espionage concerns. In May 2019, Huawei was added to the U.S. Department of

Commerce's Entity List, banning businesses without a special license. The restrictions intensified with the Federal Communications Commission (FCC)'s November 2020 rules that blocked Federal funds for purchasing equipment from companies like Huawei that were deemed national security threats. These actions were reinforced by the Secure Equipment Act of 2021, which President Joseph Biden signed, stopping the FCC from approving equipment from companies on the Covered List, including Huawei. Finally, in November 2022, the FCC banned the sale and import of new Huawei equipment, a significant measure to diminish Huawei's impact on U.S. telecom infrastructure. At the same time as it was doing this, the U.S. Government launched a diplomatic effort to persuade other nations not to buy Huawei products.

The effort, however, was too little, too late. In 1986, China had set out to overcome its concern that the United States was using its technological advantage in telecom equipment to eavesdrop on China's communications and, in the 2000s, to obviate China's ability to censor information flowing into and through the country. By 2024, the United States had no major 5G equipment manufacturers and only one factory that produced 5G equipment.[31] Huawei has become the international standard, with its equipment installed virtually everywhere worldwide that had not explicitly banned it because of national security concerns.[32]

The rise of Huawei in 5G is only part of the broader telecom narrative. For more than three decades, China has systematically employed a calculated strategy of state-driven commercial espionage and strategic technology investments across universities, laboratories, and companies to gain a significant advantage over the democratic world. At mid-decade, 5G wireless communications is illustrative of China's edge in virtually all telecom technology.

In 2024, U.S. national security concerns regarding China's telecom activities were underscored when the Federal Bureau of Investigation (FBI) and U.S. Critical Infrastructure Security Agency jointly disclosed a significant breach by China that had existed at least since 2020.[33] This cyberattack, dubbed Salt Typhoon, targeted multiple U.S. telecom companies and was characterized by U.S. officials as the most significant breach in history. It allowed Chinese access to nearly all U.S. telecom networks to monitor data traffic. Because of the inability to expel the intruders from the networks, the FBI advised Americans to encrypt communications sent through these systems. Concurrently, under a separate operation known as Volt Typhoon, China exploited its network access to infiltrate critical U.S. infrastructure, including power grids and communication systems. These hacks were possible only because of China's superb knowledge of telecom technology and almost certainly through the backdoors it had much earlier planted in telecom equipment used by U.S. telecom companies.

The immediate consequences of operations like Salt Typhoon and Volt Typhoon are significant, but the long-term effects of China's capabilities could be even more profound. China's strategy, which includes data theft as a key component, aims to secure a decisive edge in the enduring global technology race across various sectors. This strategy's success, demonstrated by China's persistent presence in U.S. telecom networks despite extensive efforts to secure them, paints a grim picture for future American technological competitiveness. As long as China maintains dominance in global telecommunications, it is likely to leverage this advantage to sustain its lead in broader technological fields.

Artificial Intelligence

Like China's telecom technology campaign, its approach to AI has deep roots. In 1986, the CCP published its 863 Program (also known as the State High-Tech Development Plan) in response to, among other things, U.S. projects like the proposed Strategic Defense Initiative. The plan aimed to boost China's technological self-reliance in strategic industries, including information technology. When U.S. companies initiated the current AI renaissance in the mid-2010s with the breakthrough in deep learning, China was quick to add this new technology to its portfolio pursued by state policy. In 2017, shortly after U.S. companies began to invest heavily in new technology, China initiated its New Generation Artificial Intelligence Development Plan, which it touted as a comprehensive blueprint to make China the global leader in AI by 2030.[34]

Like its approach to telecom technology, China's campaign to lead in this technology deployed a combination of state-driven funding, policies that promoted the emerging AI industry, and state espionage.

With regard to the first, China's government has provided substantial funding and policy support for AI start-ups, research, and major corporate players.[35] Both central and local governments have established special AI zones and created funds like the China AI Industry Development Fund, which pledged billions in initial investments.[36] These efforts are complemented by infrastructure development, including cloud computing platforms, big-data centers, and 5G networks, which serve as the backbone for AI research and deployment. Chinese universities and research institutes have also received substantial government funding to advance cutting-edge AI technologies, often in collaboration with industry leaders.[37]

China's four major tech companies—Alibaba, Baidu, Huawei, and Tencent—have benefited significantly from government support. Alibaba has leveraged government support to expand AI-powered retail, logistics, and health care applications, including the City Brain project for smart urban management.[38] Baidu has received backing for its Apollo platform, a global leader in autonomous driving research, and its contributions to smart city initiatives.[39] Huawei is a key player in AI hardware development and has received funding for projects like its Ascend AI chips, which drive AI integration in telecommunications and industrial applications.[40] Tencent, with a focus on health care AI and gaming, works closely with universities and research institutes to push for use of AI in content creation and social media.[41]

These public-private relationships have borne fruit. Start-ups benefit from tax breaks, low-interest loans, and subsidized office spaces. State-backed venture capital funds and private investors have poured significant resources into these companies, ensuring a steady stream of innovation. The government's approach promotes collaboration between public and private sectors, allowing start-ups and established companies to integrate academic research into practical applications.[42]

Regarding policies, China's government has strategically leveraged data as a resource to fuel the development of its AI industry. Its approach focuses on recognizing that access to vast and diverse datasets is key to training advanced machine-learning algorithms. This approach is underpinned by policies that encourage data-sharing and aggregation while balancing state control with public-private collaboration. This involves employing extensive

data collection mechanisms enabled by China's large population, pervasive digital infrastructure, and a centralized governance model.

A key component of this strategy is the integration of state, corporate, and individual data into comprehensive repositories. Government policies and regulations often mandate that companies, particularly in sectors like telecommunications, e-commerce, and social media, share anonymized user data for AI research and development. For example, tech giants like Alibaba, Baidu, and Tencent use their massive consumer data pools to refine AI applications in personalized advertising, logistics, and autonomous systems, often in alignment with national priorities. This symbiosis between government and industry enables the consolidation of data resources on a scale that few nations can replicate.[43]

China has actively promoted the development of "smart city" initiatives and surveillance systems, which generate an immense amount of real-time data. Projects like City Brain, implemented in cities such as Hangzhou, use data from traffic systems, public services, and urban infrastructure to optimize city management and feed AI algorithms. On the national level, data from extensive biometric surveillance networks, health records, and financial transactions is used for AI-driven governance, security, and innovation. By treating data as a strategic asset, China has positioned itself to lead in both commercial and military AI applications, ensuring that its data-driven approach remains a cornerstone of its broader technological and geopolitical ambitions.

Finally, as it did with 5G telecom technology, China has systematically employed cyber espionage to advance its AI capabilities, targeting foreign companies, universities, and government institutions. These efforts are executed through a coordinated network of state-sponsored hacking groups and human intelligence operations. A notable example is the cyber espionage campaign APT10 (Advanced Persistent Threat 10), which infiltrated major U.S. companies across sectors like aerospace, health care, and AI research.[44] These and operations like them gained unauthorized access to proprietary algorithms, datasets, and cutting-edge AI tools, enabling Chinese researchers and firms to integrate these advances into their own systems. Similarly, campaigns such as Cloud Hopper targeted managed service providers to compromise the supply chains of multiple U.S. and European technology companies.[45]

China has also used intellectual property theft to accelerate its AI development, often through the strategic use of joint ventures and forced technology transfers. Foreign firms operating in China are required to share critical technologies with local partners as part of regulatory agreements. This practice enables Chinese firms to absorb advanced techniques and implement them domestically. A well-documented case is the arrest of a former Apple engineer in 2018 who attempted to smuggle proprietary information related to Apple's autonomous vehicle project to a Chinese competitor.[46] Such instances illustrate how China leverages both institutional frameworks and individual actors to systematically acquire intellectual property essential for AI innovation.

Describing this problem, FBI Director Christopher Wray stated in a 2022 interview that the CCP has a hacking program that is bigger "than that of every other major nation combined" and that the FBI is "opening a new China counterintelligence investigation about every 12 hours," with more than 2,000 ongoing investigations.[47]

The cumulative effect of these practices has significantly bolstered China's AI industry, allowing it to compete with and, in some cases, surpass global leaders in certain fields. By reducing the time and resources required for domestic research and development, China has enhanced its capacity to innovate in areas such as autonomous driving, facial recognition, and natural language processing.

It would be difficult to know exactly what the potential of AI is for affecting the geopolitical contest between the United States and China, but several authors have made predictions. In *The Age of AI: And Our Human Future*, Henry A. Kissinger, Eric Schmidt, and Daniel Huttenlocher provide one vision when they describe the transformative potential of AI across various sectors, including business and the military. They discuss how AI can revolutionize decisionmaking processes, enhance operational efficiency, and create strategic advantages. For instance, in the business realm, AI's ability to analyze vast datasets can lead to significant breakthroughs in drug discoveries. By sifting through extensive chemical and biological data, AI can identify new molecules with potential therapeutic effects, accelerating the development of new medications and reducing research timelines. In the military domain, AI's capacity for rapid data processing and pattern recognition can enhance surveillance and reconnaissance operations. For example, AI algorithms can assist in locating and tracking stealth aircraft or submarines by analyzing anomalies in sensor data, thereby improving situational awareness and strategic response capabilities.[48]

Similarly, Mustafa Suleyman's *The Coming Wave: Technology, Power, and the 21st Century's Greatest Dilemma* delves into the potentially profound impacts of AI and other emerging technologies on society. Suleyman highlights AI's role in optimizing business operations, such as supply chain management, where predictive analytics can forecast demand fluctuations, reduce costs, and enhance efficiency. Regarding the military sphere, he discusses AI's potential to autonomously process intelligence data, identify threats, and even control unmanned systems, thereby transforming modern warfare dynamics. Suleyman underscores the dual-use nature of AI technologies, advocating for thoughtful governance to balance innovation with ethical considerations and global security.[49]

But beyond its strategic implications for digital networks, AI has critical applications in the larger realm of political warfare that absorbs much of Beijing's attention. Both companies and countries are actively developing AI tools to build psychological profiles of individuals, the first for marketing purposes and the second for repression. These tools analyze extensive datasets to conduct psychological experiments on large populations, enabling the prediction and manipulation of behavior and beliefs with remarkable precision. In the West, and the United States in particular, it is often noted that social media and news-related AI algorithms have played a large role in polarizing the public into distinct antagonistic political camps. In China, the CCP has harnessed AI to do the opposite, attempting to target domestic and foreign consumers so that they receive only information that unifies them behind the Party. Besides making domestic repression more effective internationally, this technology can potentially replace the hundreds of thousands of blundering "50-centers" described earlier with a handful of potentially highly effective AIs.

What may be most important, however, is the role of AI in China's longer-term information strategy. Among AI's uses is cyber security. If the CCP is correct in viewing the information sphere as the primary locale of Great Power competition in the digital age, AI

will play a significant role in future geopolitics because it is one of the key weapons Great Powers use to attempt to manipulate and control the global flow of digital information. Recently, the FBI warned of increasing use of AI in cyberattacks.[50] Over time, AI will play an increasingly large role in both cyber offense and defense, potentially providing a significant advantage in the digital arms race to nations with an advantage in this area.

Quantum Technology

The third major technology China is attempting to lead is quantum computing. Quantum machines are theoretically capable of performing computations at speeds vastly exceeding those of conventional computers and promise to disrupt the foundation of cybersecurity. Historically, quantum computing has been a distant aspiration, but recent advancements have brought it closer to reality. Companies like IBM and Google have developed early-stage quantum computers that showcase the technology's immense potential. While these machines have so far demonstrated only limited capability to break encryption, experts agree that such capabilities are on the horizon. Recent breakthroughs have created an intense international race, not only to develop quantum technology but also to counter its risks.[51]

The primary threat posed by quantum computing lies in its ability to render current encryption methods obsolete. Modern encryption secures everything from financial transactions to military communications, and in many cases, encryption serves as the single point of failure in digital systems. Quantum computers, with their ability to solve complex mathematical problems exponentially faster than classical computers, could decrypt encrypted data amassed over decades. This would expose confidential communications, industrial secrets, and sensitive national security information, fundamentally altering the cyber landscape.[52]

The implications of this breakthrough would not be evenly distributed. Western industries and militaries that rely on encryption to secure operations and communications would be disproportionately affected. By contrast, nations with less dependence on encryption, such as China, could gain a strategic advantage in cyberspace through quantum decryption.

China has aggressively pursued quantum technology, investing approximately $15 billion into quantum research and development.[53] This investment significantly outpaces U.S. public-sector spending. China's focus on quantum communications, including its development of the world's largest quantum communication network, demonstrates its strategic commitment to leading in this domain.[54]

While the United States currently leads in quantum computing, thanks to the innovation of private-sector leaders like IBM and Google, China's state-driven approach aims to close the gap. If China achieves quantum supremacy (the ability to use quantum computing to break current encryption) first, it will gain unparalleled capabilities to decrypt critical systems, steal industrial secrets, and compromise its adversaries' civilian and military networks.

Recognizing the threat posed by quantum decryption, researchers and policymakers in the West are racing to develop quantum-resistant encryption methods, often referred to as postquantum cryptography. These encryption techniques rely on mathematical problems that are resistant to quantum attacks. In 2022, the U.S. National Institute of Standards and Technology finalized its initial selection of quantum-resistant encryption algorithms. These

algorithms are being integrated into new cryptographic standards to safeguard critical infrastructure, financial systems, and military communications. However, the challenge lies in deploying these new standards at scale before quantum decryption becomes a practical reality. The process of transitioning global systems to postquantum encryption is complex, resource-intensive, and time-sensitive. The window of opportunity to secure critical information before quantum decryption becomes viable is closing, but how much time remains is anyone's guess.[55]

Countering China's Strategy

In countering China's technology-based information strategy, the first thing that the West must come to terms with is that China is currently winning. According to the Australian Strategic Policy Institute, between 2007 and 2022, China went from leading scientific and research innovation in 3 of 64 critical technologies to 57 of 64. During the same period, the United States moved from leading in 60 to 7.[56] These statistics oversimplify a complex issue.[57] China's advances are also closely tied to foreign technologies and supply chains and depend on stolen Western technology.[58] But the more significant problem is not that Americans exaggerate China's growing dominance; instead, it is that American leaders are prone to bury their heads in the sand and believe that the U.S. technological advantage that dominated their youth continues to exist today. That the CCP hopes to encourage this ostrich-like view is borne out by its efforts to suppress or counter empirical evidence of China's technological growth. For instance, some of the most readily available online evidence that China is not winning tends to come from publications by CCP-leaning news sources, institutions, and authors.[59]

Fortunately, among the handful of technology areas that the United States continues to lead are cybersecurity, AI, and quantum computing.[60] So long as the West can still compete in these information-control technologies, there is some hope that it can prevent absolute Chinese tech supremacy. The United States, along with the broader democratic world, lags significantly behind China in technological research. Given that the U.S.-led liberal international order relies on democracies maintaining a technological edge over autocratic regimes, the present situation is deeply concerning.

The second uncomfortable fact the United States must come to terms with is that under the best-case scenario, the current technological contest will be generational. China has spent the past three decades investing heavily in science, technology, engineering, and mathematics education and building a workforce capable of competing in the tech arena, while the United States has not. Winning a technological race will necessitate, above all, building a U.S. workforce capable of competing—and that will require decades. Additionally, from the outset, China's government has treated technology as a strategic asset. During the Cold War, the United States held this outlook, but after the Soviet Union fell, it abandoned this perspective in favor of an optimistic version of globalism that included turning a blind eye to IP theft and backing transfers of economic and military technologies (see table). Addressing the current situation will require a new model of government-led investing in technologies appropriate to the current contest with China.

Third, the United States must acknowledge that borderless cyber flows no longer consistently work to its advantage. In the aftermath of the Cold War, the United States could

safely champion a less-global Internet because there was no Great Power capable of exploiting this to the detriment of the free world and because it could assume, based on its Cold War experience, that a borderless flow of information would work wholly in its geopolitical favor. These assumptions are clearly no longer true. The United States faces a Great Power adversary that is capable and willing to use the lack of cyber borders in Western nations to steal from and sabotage their private industry and militaries.

Considering these technology-induced geopolitical changes, the United States must develop a new approach to controlling the cyber domain based on the idea that geopolitical competition is today as much about controlling digital networks as about controlling physical space. In the past, the central conflict in Great Power politics involved control of physical territory because this was how countries produced wealth. To this end, nations developed and deployed bases, fleets, and bombers. While these older instruments of national power continue to be critical, the game has changed. Today, the key to Great Power politics is control of information and the networks on which information flows. China did not transition from its 20th-century position as a failing developing nation in which tens of millions of people starved to death every few decades to its status as a relatively wealthy superpower by conquering territory. It did so in no small measure by conquering digital networks.

To transition to a digital-age competitive mentality and Great Power force posture, the United States must refocus its capabilities on winning the contest to control digital networks. This will require moving resources from traditional forms of power to those that allow the United States and its democratic allies more influence on global information flows. It will also require two other actions.

The first is well-rehearsed and accepted by large parts of the U.S. Government. Keeping up with China in terms of technology will require investments in the development and commercial deployment of 5G wireless, AI, and quantum computing. This means providing funds and subsidies for friendly companies developing 5G and 6G wireless and other telecom equipment. It will involve enabling the financing of telecom infrastructure abroad as a counter to China's efforts. It will also require investments, incentives, and legislation designed to mitigate the national security impact of China's use of AI and quantum technologies for global information control.[61]

The second step, however, is equally important but significantly more controversial. China has used IT and policies related to its Great Firewall system to surround itself with an information fortress to hide within as it relentlessly attacks the West. If these attacks are left unanswered, there can be no doubt that China will eventually win the information war. When it does, it will gain a potentially insurmountable advantage when it comes to setting the rules for the global international order.

To prevent this outcome, the United States and its allies must cut off China's access to many Western information systems. There is no simple or prescriptive way to accomplish this end. However, it will involve changing the Western mindset that views digital connections with geopolitical adversaries as free speech. This does not mean that U.S. citizens should not have access to Chinese information. What it does mean, however, is that when a digital connection provides Chinese agents with the ability to hack into systems, steal information, or sabotage, it should be cut off. Legally and technically, removing Chinese

access to U.S. and potentially Western networks must be a critical priority for U.S. policy before the end of the decade.

Just as Chinese citizens need visas to enter the United States physically, they should provide a digital equivalent to access the Internet of free nations, ensuring accountability for their actions. While this system would be imperfect and demand significant technological advancements, it could help mitigate risks.

There is an argument that given China's lead in most technologies, it is too late to employ such a digital throttling strategy against its information operations. While there is something to this argument, it is also true that China's domestic scientific institutions developed out of a system based almost entirely on digesting stolen intellectual property and that they still rely heavily on this approach. Reducing the flow of science and technology to Chinese institutions by technical and legal means would significantly reduce their capability to innovate. In a world without IP theft, it would likely take years or decades for China to redesign its technology institutions to work as well as they do now. Furthermore, while it is true that reducing China's access to U.S. networks would also reduce U.S. access to Chinese networks, the problem would be vastly less grave for U.S. researchers because China already prevents its scientists from sharing most new technology outside its borders.

Conclusion

The United States is currently enmeshed in a Great Power competition different from any the world has experienced. In the past, Great Powers fought over control of continents and oceans. In the current contest, the United States and China compete to control digital networks and information.

This chapter mainly focuses on three technologies: 5G wireless, AI, and quantum computing technologies. While each of these is independently important, their greater importance in the context of Great Power competition involves how they are allowing China to control global information. To the extent that China can continue to use its control of the world's information to pirate technology, winning in these technologies means winning in many others. So long as China can use its IT advantage to shield its population from Western ideas while conducting political operations and critical infrastructure sabotage outside its borders, it will remain on track to undermine and eventually replace the U.S.-led international order.

It is still possible to prevent China from leveraging its geopolitical information strategy to solidify its position as the world leader. While by some measures China currently surpasses the United States in scientific research across 90 percent of critical technologies, by acting strategically, the United States can disrupt PRC momentum and prevent it from turning this lead into global dominance. Countering China's ability to reshape the global order through its technological advantage will require strategic efforts to address its vulnerabilities. Chief among these is its reliance on IP theft from the West—a critical weakness that can be exploited.

Halting the illegal transfer of technology to China is imperative but will demand a significant shift in perspective. Intellectual property theft must be treated with the same seriousness as physical theft. Criminals who have repeatedly been caught stealing are seldom given free access to the houses they burgle, and China's access to U.S. digital networks

should be treated accordingly. Most important, there must be a clear recognition that the United States is engaged in a high-stakes competition with China for global influence. If the United States is to avoid geopolitical failure, it must prioritize technologies and policies designed to prevent China from achieving control over the global flow of information through the domination of digital networks.

Notes

[1] Richard Andres, "Emerging Critical Information Technology and Great Power Competition," in *Strategic Assessment 2020: Into a New Era of Great Power Competition*, ed. Thomas F. Lynch III (Washington, DC: NDU Press, 2020), 139–52, https://ndupress.ndu.edu/Publications/Books/Strategic-Assessments-2020/.

[2] See Xuan-Thao Nguyen, "Tech Supremacy: The New Arms Race Between China and the United States," *Journal of Corporate Law* 49, no. 1 (2023), 103–36, https://jcl.law.uiowa.edu/sites/jcl.law.uiowa.edu/files/2023-11/Nguyen_Final.pdf; David Matthews, "U.S. Holds Off China Challenge in Global R&D Spending Race," *Science/Business*, March 14, 2024, https://sciencebusiness.net/news/international-news/us-holds-china-challenge-global-rd-spending-race; David C. Gompert, "Winning the U.S.-China Technology Race," *Survival* 66, no. 4 (2024), 77–84, https://doi.org/10.1080/00396338.2024.2380198; Chi Lo, "The China-U.S. Tech Race," *China's Global Disruption: Myths and Reality* (Bradford, UK: Emerald Publishing Limited, 2021), 39–51.

[3] Jennifer Wong Leung et al., *ASPI's Two-Decade Critical Technology Tracker: The Rewards of Long-Term Research Investment* (Canberra: Australian Strategic Policy Institute [ASPI], August 2024), https://www.aspi.org.au/report/aspis-two-decade-critical-technology-tracker.

[4] Leung et al., *ASPI's Two-Decade Critical Technology Tracker*.

[5] For work on this topic, see Qingmin Dai, "Innovating and Developing Views on Information Operations," *Beijing Zhongguo Junshi Kexue*, August 20, 2000, 72–77 (translated and downloaded from Foreign Broadcast Information Service, November 9, 2000); Timothy Lloyd Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice From 1995–2003* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), https://archive.org/details/Dragon_Bytes_Chinese_Information_War_Theory_and_Practice_Timothy_L._Thomas.

[6] "Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference," DigiChina, April 30, 2018, https://digichina.stanford.edu/work/translation-xi-jinpings-april-20-speech-at-the-national-cybersecurity-and-informatization-work-conference/.

[7] Ian Sullivan, "China and Russia: Achieving Decision Dominance and Information Advantage," *Mad Scientist Laboratory*, November 1, 2021, https://madsciblog.tradoc.army.mil/364-china-and-russia-achieving-decision-dominance-and-information-advantage/; Dean Cheng, "How China Seeks to Dominate the Information Age," United States Institute of Peace, March 7, 2024, https://web.archive.org/web/20240614003826/https://www.usip.org/publications/2024/03/how-china-seeks-dominate-information-age.

[8] David Rothkopf, *Running the World: The Inside Story of the National Security Council and the Architects of American Power* (New York: PublicAffairs, 2009), 350; James Mann, *About Face: A History of America's Curious Relationship With China, From Nixon to Clinton* (New York: Knopf, 1999), chap. 16.

[9] Karen M. Sutter and Emily G. Blevins, *U.S. China Science and Technology Cooperation Agreement*, IF12510 (Washington, DC: Congressional Research Service, Updated December 13, 2024), https://crsreports.congress.gov/product/pdf/IF/IF12510.

[10] See "Marshall Plan (1948)," National Archives, n.d., https://www.archives.gov/milestone-documents/marshall-plan.

[11] Millennium Challenge Corporation, *Freedom of Information Indicator*, n.d., https://www.mcc.gov/who-we-select/indicator/freedom-of-information-indicator; David Dollar and Aart Kraay, "Trade, Growth, and Poverty," *Finance & Development* 38, no. 3 (September 2001), https://www.imf.org/external/pubs/ft/fandd/2001/09/dollar.htm.

[12] Laura Solanko, *From Reform to Stagnation—20 Years of Economic Policies in Putin's Russia*, BOFIT Policy Brief No. 1 (Helsinki: Bank of Finland, 2020), 9, https://publications.bof.fi/bitstream/handle/10024/44875/bpb0120.pdf.

[13] Thomas, *Dragon Bytes*.

[14] For an overview of this campaign, see *Update to the Section 301 Report: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* (Washington, DC: Office of the United States Trade Representative, November 20, 2018), https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf.

[15] Birol Akduman, "From the Great Wall to the Great Firewall: A Historical Analysis of China's Surveillance Apparatus," *International Journal of Social Sciences* 7, no. 28 (2023), 293–319, https://doi.org/10.52096/usbd.7.28.21.

[16] *How the People's Republic of China Seeks to Reshape the Global Information Environment*, Global Engagement Center Special Report (Washington, DC: Department of State, 2023), https://web.archive.org/web/20231001025544/https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/.

[17] *Report of the Select Committee on U.S. National Security and Military/Commercial Concerns With the People's Republic of China* (Washington, DC: Government Printing Office, May 25, 1999), https://www.congress.gov/congressional-report/105th-congress/house-report/851/1.

[18] *Findings of the Investigation Into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974* (Washington, DC: Office of the United States Trade Representative, 2018), 11–14, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[19] *Report of the Select Committee on U.S. National Security and Military/Commercial Concerns With the People's Republic of China*.

[20] See, for instance, Jamie M. Ellis, "Chinese Cyber Espionage: A Complementary Method to Aid PLA Modernization" (Master's thesis, Naval Postgraduate School, December 2015), https://apps.dtic.mil/sti/tr/pdf/ADA632209.pdf; Bryan Krekel,

Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation (McLean, VA: Northrup Grumman Corporation, October 9, 2009), https://nsarchive.gwu.edu/document/21426-document-30.

[21] Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House, May 29, 2009, https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[22] Akduman, "From the Great Wall to the Great Firewall."

[23] Ai Weiwei, "China's Paid Trolls: Meet the 50-Cent Party," *New Statesman*, October 25, 2012, https://www.newstatesman.com/long-reads/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party.

[24] For a discussion of U.S. business response to hacking in this era, see Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (New York: Penguin, 2019), chap. 5.

[25] For insights into China's approach, see, for instance, "Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference."

[26] Del Quentin Wilber, "China's High-Tech Spying Surges," *Los Angeles Times*, n.d., https://enewspaper.latimes.com/infinity/article_share.aspx?guid=14f1f59d-4c55-4f71-bb5c-e357925c9f48; Karen M. Sutter, *Made in China 2025 and Industrial Policies: Issues for Congress*, IF10964 (Washington, DC: Congressional Research Service, Updated December 12, 2024), https://www.congress.gov/crs-product/IF10964.

[27] Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 25, 2019.

[28] Michael G. McLaughlin and William J. Holstein, *Battlefield Cyber: How China and Russia Are Undermining Our Democracy and National Security* (Lanham, MD: Prometheus Press, 2023).

[29] McLaughlin and Holstein, *Battlefield Cyber*.

[30] McLaughlin and Holstein, *Battlefield Cyber*, chap. 3.

[31] Ike Brannon, "Boosting Domestic Production of 5G Technology Is Important to Ensure Long Run U.S. Economic Primacy," *Forbes*, September 26, 2022, https://www.forbes.com/sites/ikebrannon/2022/09/26/boosting-domestic-production-of-5g-technology-is-important-to-ensure-long-run-us-economic-primacy/; "JMA Receives $44 Million in Federal Funding to Boost State-of-the-Art 5G Manufacturing Facility in Syracuse," JMA, n.d., https://jmawireless.com/jma-receives-44-million-in-federal-funding-to-boost-state-of-the-art-5g-manufacturing-facility-in-syracuse/.

[32] Thomas Donahue, "The Worst Possible Day: U.S. Telecommunications and Huawei," *PRISM* 8, no. 3 (2020), 15–35, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2053215/the-worst-possible-day-us-telecommunications-and-huawei/.

[33] "Joint Statement From FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure," Cybersecurity and Infrastructure Security Agency, November 13, 2024, https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications.

[34] Daniel S. Hoadley, *Artificial Intelligence and National Security*, R45178 (Washington, DC: Congressional Research Service, November 10, 2020), https://crsreports.congress.gov/product/pdf/R/R45178.

[35] Ngor Luong and Margarita Konaev, "In and Out of China: Financial Support for AI Development," Center for Security and Emerging Technology at Georgetown University, August 10, 2023, https://cset.georgetown.edu/article/in-out-of-china-financial-support-for-ai-development/.

[36] "17 AI Pilot Zones Built in China," State Council of the People's Republic of China, December 6, 2021, https://english.www.gov.cn/statecouncil/ministries/202112/06/content_WS61ae0e58c6d09c94e48a1c59.html.

[37] Du Juan, "Beijing Goes All Out to Fund AI Tech," *China Daily*, March 1, 2024, https://www.chinadaily.com.cn/a/202403/01/WS65e12a0fa31082fc043b9e8b.html.

[38] Abigail Beall, "In China, Alibaba's Data-Hungry AI Is Controlling (and Watching) Cities," *Wired*, May 30, 2018, https://www.wired.com/story/alibaba-city-brain-artificial-intelligence-china-kuala-lumpur/.

[39] "Baidu's Autonomous Driving Solutions Make Significant Strides, Aiming to Cover 65 Cities by 2025 and Leading in China's Mobility Revolution," *GlobeNewswire*, September 15, 2023, https://www.globenewswire.com/news-release/2023/09/15/2743780/0/en/Baidu-s-Autonomous-Driving-Solutions-Make-Significant-Strides-Aiming-to-Cover-65-Cities-by-2025-and-Leading-in-China-s-Mobility-Revolution.html; Mai Tao, "Baidu Launches 'World's First' Multi-Modal Autonomous Driving Mobility-as-a-Service Platform," *Robotics and Automation News*, February 9, 2021, https://roboticsandautomationnews.com/2021/02/09/baidu-launches-worlds-first-multi-modal-autonomous-driving-mobility-as-a-service-platform/40316/.

[40] Reuters, "Exclusive—Huawei Aims to Mass-Produce Newest AI Chip in Early 2025, Despite U.S. Curbs, Sources Say," *U.S. News & World Report*, November 21, 2024, https://money.usnews.com/investing/news/articles/2024-11-21/exclusive-huawei-aims-to-mass-produce-newest-ai-chip-in-early-2025-despite-us-curbs.

[41] Anubhav, "Tencent's Big Move into AI-Enhanced Healthcare in China," *Gizmochina*, November 22, 2023, https://www.gizmochina.com/2023/11/22/tencent-ai-healthcare-china/; June Yoon, "AI Could Actually Change the Gaming Industry," *Financial Times*, August 18, 2024,.

[42] Liza Lin and Rebecca Feng, "For Chinese Tech Startups, Beijing Fills a Funding Void Left by VCs," *Wall Street Journal*, October 3, 2024; Joe Leahy and Tina Hu, "China Gets Creative to Boost Lending to Tech Start-Ups," *Financial Times*, August 19, 2024.

[43] Winston Ma, "China's Approach to Data and AI Is Changing. Here's What That Means," World Economic Forum, January 11, 2024, https://www.weforum.org/stories/2024/01/chinas-data-and-ai-approach-is-changing-heres-what-that-means/.

[44] Brian Barrett, "How China's Elite Hackers Stole the World's Most Valuable Secrets," *Wired*, December 20, 2018, https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/.

[45] Jack Stubbs et al., "Inside the West's Failed Fight Against China's 'Cloud Hopper' Hackers," Reuters, June 26, 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.

[46] "U.S. Charges Four Over China 'Operation Fox Hunt' Pressure Campaign," BBC News, May 17, 2023, https://www.bbc.com/news/world-us-canada-65616384.

[47] Scott Pelley, "FBI Director Christopher Wray on Foreign Cyberattacks, Domestic Terrorism," CBS News, April 24, 2022, https://www.cbsnews.com/news/fbi-director-christopher-wray-60-minutes-2022-04-24/.

[48] Henry A. Kissinger et al., *The Age of AI: And Our Human Future* (New York: Little, Brown and Company, 2021).

[49] Mustafa Suleyman, *The Coming Wave: Technology, Power, and the Twenty-First Century's Greatest Dilemma*, with Michael Bhaskar (New York: Crown, 2023).

[50] "FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence," Federal Bureau of Investigation, May 8, 2024, https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence.

[51] Benjamin Pimentel, "SAP CEO Sees Huge Quantum Computing Impact in 3 to 4 Years," *Investor's Business Daily*, January 14, 2025, https://www.investors.com/news/technology/quantum-computing-sap-ceo-impact/.

[52] Travis Scholten et al., "Assessing the Benefits and Risks of Quantum Computers," *IEEE Security & Privacy*, July 17, 2024, https://www.nist.gov/publications/assessing-benefits-and-risks-quantum-computers; "DHS Releases Guidance to Mitigate Security Risks From the Advancement of Quantum Computing," Department of Homeland Security, October 4, 2021, https://www.dhs.gov/news/2021/10/04/dhs-releases-guidance-mitigate-security-risks-advancement-quantum-computing.

[53] Jakob Pii, "Chinese Quantum Companies and National Strategy 2023," *Quantum Insider*, April 13, 2023, https://thequantuminsider.com/2023/04/13/chinese-quantum-companies-and-national-strategy-2023/.

[54] Paul Smith-Goodson, "Quantum USA vs. Quantum China: The World's Most Important Technology Race," *Forbes*, October 10, 2019, https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race.

[55] Richard Tyler, "Battle Begins to Stop Quantum Computers Smashing Cyber Defences," *The Times* (London), August 20, 2024, https://www.thetimes.com/business-money/entrepreneurs/article/battle-begins-to-stop-quantum-computers-smashing-cyber-defenses-rzmlwqw7f.

[56] Leung et al., *ASPI's Two-Decade Critical Technology Tracker*.

[57] See, for instance, David Lin et al., *Welcome to the Arena: Who's Ahead, Who's Behind, and Where We Are Headed Next in the U.S.-China Technology Competition*, 2025 Gaps Analysis (Arlington, VA: Special Competitive Studies Project, January 2025), https://www.scsp.ai/reports/2025-gaps-analysis/.

[58] Otaviano Canuto and Antônio Jorge Martins, *The Automotive Transition on the Road to Decarbonization*, Policy Brief No. 51 (Rabat, Morocco: Policy Center for the New South, October 2024), https://www.policycenter.ma/sites/default/files/2024-10/PB_51-24_Canuto%20%26%20Antonio%20jorge.pdf; Claris Diaz, "Artificial Intelligence as an Indirect Threat: Disruptive Applications to Food Security and Implications for the Geopolitical Order" (Master's thesis, Jagiellonian University, 2024), https://web.archive.org/web/20250814012516/https://ruj.uj.edu.pl/handle/item/382805; Greg Austin, "The Problem With China's Patents," *The Diplomat*, March 3, 2015, https://thediplomat.com/2015/03/the-problem-with-chinas-patents/.

[59] Marina Yue Zhang, "Chinese Tech Dominance More Myth Than Reality," *East Asia Forum*, April 21, 2023, https://www.eastasiaforum.org/2023/04/21/chinese-tech-dominance-more-myth-than-reality/; Zhang Xi, "Australian Think Tank Biased on China's Technology Progress," *China Daily*, March 3, 2023, https://www.chinadaily.com.cn/a/202303/03/WS6401d572a31057c47ebb20ca.html.

[60] Other sources reinforce that the United States continues to lead in these areas. The United States has traditionally kept a small but important lead in AI. However, this lead is sometimes measured in months rather than years. See, for instance, "Tech Stocks Tumble as DeepSeek Debuts a Cheap Chinese AI Model," *Economist*, January 28, 2025, https://www.economist.com/podcasts/2025/01/28/tech-stocks-tumble-as-deepseek-debuts-a-cheap-chinese-ai-model. For the longer view, see Eric Schmidt, chairman, et al., *National Security Commission on Artificial Intelligence: Interim Report* (Washington, DC: National Security Commission on Artificial Intelligence, November 2019), 435; Jungsang Kim and Christopher Monroe, "America Is the Undisputed World Leader in Quantum Computing Even Though China Spends 8x More on the Technology—But an Own Goal Could Soon Erode U.S. Dominance," *Fortune*, April 12, 2024, https://fortune.com/2024/04/12/america-undisputed-world-leader-quantum-computing-even-though-china-spends-technology-us-dominance/.

[61] Schmidt, chairman, et al., *National Security Commission on Artificial Intelligence*, chap. 11.