

The Determining Elements of the New Great Power Competition

Unpacking the Race for Technological Supremacy

By Ronen Medzini

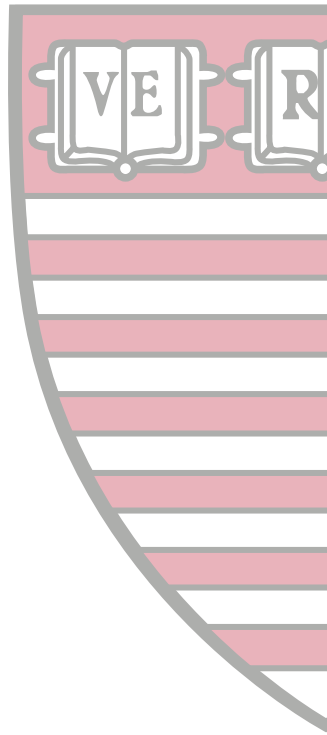
Fellow at the Rajawali Foundation Institute for Asia, China Public Policy Program

November 2024



HARVARD Kennedy School

RAJAWALI FOUNDATION INSTITUTE FOR ASIA



The Determining Elements of the New Great Power Competition

Unpacking the Race for Technological Supremacy

By Ronen Medzini

Fellow at the Rajawali Foundation Institute for Asia, China Public Policy Program

About the Rajawali Foundation Institute for Asia

The Rajawali Foundation Institute for Asia is housed at the Ash Center for Democratic Governance and Innovation, one of twelve research centers at Harvard Kennedy School. In 2008, under the leadership of Anthony Saich, the Asia Programs at HKS (now the Rajawali Foundation Institute for Asia) joined the Ash Institute for Democratic Governance and Innovation. Two years later, the permanently endowed Rajawali Foundation Institute for Asia was established as part of the Ash Center to bring together academics and practitioners from around the world to enhance research, teaching, and training on public policy and governance issues of critical importance in Asia.

About the Ash Center for Democratic Governance and Innovation

The Roy and Lila Ash Center for Democratic Governance and Innovation advances excellence and innovation in governance and public policy through research, education, and public discussion. By training the very best leaders, developing powerful new ideas, and disseminating innovative solutions and institutional reforms, the Center's goal is to meet the profound challenges facing the world's citizens. The Ford Foundation is a founding donor of the Center. Additional information about the Ash Center is available at ash.harvard.edu.

The views expressed in this paper are those of the author(s) and do not necessarily reflect those of the John F. Kennedy School of Government or of Harvard University. Papers are intended to elicit feedback and to encourage debate on important public policy challenges.

This paper is copyrighted by the author(s). It cannot be reproduced or reused without permission. Pursuant to the Ash Center's Open Access Policy, this paper is available to the public at rajawali.hks.harvard.edu free of charge.

A PUBLICATION OF THE

Rajawali Foundation Institute for Asia

Harvard Kennedy School

79 John F. Kennedy Street

Cambridge, MA 02138

rajawali.hks.harvard.edu

Contents

Executive Summary.....	1
Great Power Competition: Introduction.....	3
The Shifting Concept of Power: Technology as the New Ideology.....	4
Power-Defining Technologies: A Comparative Analysis.....	7
“In Modern Warfare, Victory Hinges on Information”.....	9
TikTok, Encryption, and Human Cognition: New Technological Battlefields.....	12
Makers, Takers, and Laggards: A First-Mover Race to Reshaping Societies and Economies.....	16
Biopower: Hacking Life, Fostering Discoveries, and Shaping Generations.....	21
One World, Two Systems: The Inevitable Path to Technological Decoupling.....	24
Conclusion.....	26
Appendix A: CETs Classifications in the US and China.....	28
Notes.....	29

Executive Summary

At present, momentous changes of a like not seen in a century are accelerating across the world. A new round of scientific and technological revolution and industrial transformation is well under way, and a significant shift is taking place in the international balance of power, presenting China with new strategic opportunities in pursuing development.

—Xi Jinping to the 20th National Congress of the Communist Party of China,
October 16, 2022

The contemporary competition between the United States and China, though echoing past dynamics of the Cold War, reveals significant shifts in the defining elements of “great power.” Unlike the ideological rivalry between the US and the Soviet Union, which previously divided the world into two blocs, today’s global power relations hinge on technological superiority and are driven by alliances, data, and resource control. However, the categorizations and definitions of the technologies deemed “strategic” remain dynamic and subject to diverging perceptions.

This research paper seeks to bridge the gap between policymakers and technology experts by deciphering the determinants of modern technological competition. It sets the stage by identifying the main disparities between the Cold War era and the present bipolar rivalry and articulates new foundational elements that define “great powers” today. Subsequently, the paper delves into the varied components of critical technologies; elucidates their core attributes; evaluates their implications across national security, commercial, and societal domains; and unpacks the strategic factors for attaining technological superiority. Five principal insights are drawn from this analysis, which are sequentially presented as follows:

1. **The role of alliances:** As great powers rely on adherence to a particular world order that they endorse, a fundamental aspect of their competition involves the formation of alliances. Whereas alliances during the Cold War were delineated along ideological lines, forming distinct blocs, contemporary global rivalries feature more flexible, interest-based alliances that do not preclude competitive interactions among nations. As the race of technological superiority hinges on multinational cooperation, the US may be underutilizing one of its significant strategic advantages: forming value-based alliances rooted in democratic principles.
2. **The essence of technologies in comprehensive power:** A comparative analysis of how the US and China conceptualize technological supremacy illustrates differing national priorities. The US predominantly frames it within the context of national security, incorporating military technologies into its list of critical emerging technologies. In contrast, China perceives technological supremacy as an avenue for asserting global economic leadership, deliberately omitting military applications in

its strategic documents and instead highlighting fields such as genetic editing and synthetic biology.

3. **Transforming national security concepts:** The integration of emerging technologies into contemporary warfare signifies an evolutionary development, not a revolutionary shift. However, in a context defined by pervasive global digital dependency and connectivity, the significance of data and the impact of nonlethal capabilities—such as cyber warfare and social media influence campaigns—have begun to eclipse traditional physical military actions. These nonlethal strategies are increasingly influential, extending their effects beyond the battlefield into societal, political, and cognitive domains.
4. **Reshaping societies as a whole:** The quest for technological hegemony is primarily driven by the pursuit of commercial and societal dominance. Pioneers in crucial technological domains are poised to secure market dominance, influence the creation of international standards, and redefine the global economic hierarchy, distinguishing between leaders, followers, and laggards. Among various critical emerging technologies, artificial intelligence (AI) and biotechnology are particularly noteworthy. These general-purpose technologies have the potential to fundamentally transform the global order, shift the balance of power, and significantly impact daily life.
5. **An inevitable path to tech decoupling:** As the contest for technological preeminence intensifies, two incompatible technological ecosystems are crystallizing. In this evolving landscape, third countries may find themselves inevitably forced to align with one of the two opposing technological factions, thereby potentially redividing the world into distinct technological blocs.

Great Power Competition: Introduction

A state of “Great Power Competition” (GPC) infers an ongoing geopolitical rivalry between two or more parties of comparative scale, each striving to shape and dominate the world order. While the term “competition” implies an outcome of winners and losers, its end game is by no means decisive. Rather, it is a long-term struggle, often between rising and descending powers, over spheres of influence and the setting of global economic and political infrastructure in a favorable manner to support and extend their overarching national strength.

From an economic perspective, a great power’s influence extends beyond its wealth and financial indicators. It encompasses predominance in global financial markets, reserve currencies, banking systems, and multilateral financial institutions. Politically, great powers wield considerable diplomatic weight in shaping contemporary international affairs and hold sway over international institutions and global governance structures. Military might, by itself, is not the essence of the competition but rather the means to project power, uphold the current international order, or challenge it.

A great power relies on compliance with a certain world order, and a state of competition entails alternatives to the reigning order, offering countries to reposition existing patron-client relations and overall allegiances. Subsequently, a key characteristic of competitions between powers is the formation of alliances, which may range in scope from limited cooperation (e.g., exclusive trade agreements) to strategic frameworks (e.g., bilateral military exchanges, regional and multilateral security networks), and hermetic blocs—coalitions of countries willing to compromise various national sovereignties for pursuing a greater joint interest.

In correlation with globalization and modernization, great powers rely on effective alliances in their endeavor to obtain the most advanced technological and military capabilities and extend their global influence. In principle, these great power alliances are built on shared interests and values. From the perspective of interests, a country might align itself with a great power to benefit from security guarantees, economic assistance, or political support. In return, a great power seeks geopolitical gains to reinforce its dominance in forms such as overseas military presence, intelligence sharing, technological exchanges, access to markets and resources, and limitation of economic and technological cooperation with rivaling great powers.

The second pillar of alliances revolves around shared values, which can extend from specific mutual principles, such as human rights or anti-imperialism, to a broader comprehensive worldview, namely ideology. While interest-based alliances are often as strong (or fragile) as the ability and will to satisfy their underlying guarantees, ideological alliances tend to foster deeper, more enduring, and intimate cooperation, promoting greater alignment with a great power’s vision of world order.

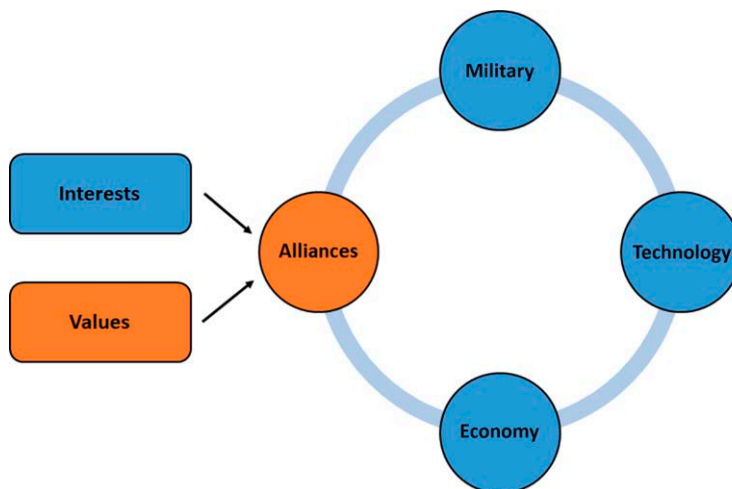
Nevertheless, in a moderate-scale GPC, interest-based alliances often prevail over ideological ones. A country's strategic dependency on a non-like-minded great power, for example, is likely to affect its willingness to actively align with rivaled interest-based alliances that might, as a result, jeopardize its national security, energetic and economic resilience, or political stability. Moreover, it is in a country's interest to stretch its diplomatic web and maximize its economic potential by cooperating with all willing counterparts, regardless of their domestic policies and geopolitical aspirations. It is only when the competition is perceived as existential or escalates in magnitude to a recognized state of a "cold war" that countries are compelled to strategically "choose sides," and would likely favor value-based alliances over short- to mid-term interests.

The Shifting Concept of Power: Technology as the New Ideology

Historically, values—or, more precisely, ideologies—were the driving force of power relations and primary parameter of national security during the Cold War. The "Red Scare" of increasing Soviet influence in Europe and Asia and of domestic cells of espionage resulted in the US policy of "containment" against the spread of communist ideology.¹ Similarly, the USSR considered its post-war Eastern European satellite states as physical and ideological barriers against capitalist influence,² fearing an inverse domino effect scenario in which, as articulated in the Brezhnev Doctrine, "the weakening of any of the links in the world system of socialism directly affects all the socialist countries."³

While the struggle for dominance during the Cold War manifested in an arms race, technological competition, espionage, trade embargoes, and information warfare, ideology was the *de facto* element that defined alliances, shaped the balance of power, and was critical enough for great power leaders to send troops overseas. Evidently, fear of regime changes were the *casus belli* for the US in Korea (1950–1953) and Vietnam (1964–1973), as well as for the Soviet Union–led Warsaw Pact invasion of Czechoslovakia (1968) and its war in Afghanistan (1979–1989).

The era was marked by the emergence of two distinct ideological blocs, pitting the efficacy of socialist and capitalist economies, and democratic and communist governance systems, against each other. In this geopolitical landscape, comprehensive power was defined through the interplay of alliances, economic resilience, military strength, and technological supremacy, as depicted in Figure 1. Among these elements, alliances became the critical lever for the two superpowers to influence the balance of power, as the advent of nuclear weapons and the doctrine of "mutually assured destruction" (MAD) deterrence reduced the militaries' roles toward power projection and conventional proxy wars. Furthermore, the capability to impede economic and technological progress through coercion or sanctions was limited, as the two blocs were effectively insulated within their respective ecosystems.

Figure 1. The Defining Elements of Power during the Cold War

While the emerging GPC between the US and China shares several similarities with the Cold War era, the dynamics of power creation, projection, and reinforcement have evolved. First, the role of ideology in shaping alliances has significantly diminished. While the US remains committed to promoting democratic ideology and values abroad,⁴ and establishes new exclusive security pacts with other democracies,⁵ China’s global vision does not include spreading Communism, “Socialism with Chinese Characteristics,” or “Xi Jinping Thought,” which remain primarily domestic doctrines. Furthermore, China’s foreign and defense policies advocate “partnerships” over “alliances,”⁶ with the vast majority of these partnerships clearly being interest-based rather than ideological. A contemporary example of this reduced emphasis on ideology is the military cooperation between the US and its former foe Vietnam—by definition, a communist country.⁷

The second significant difference is the geopolitical framework. The US and the Soviet Union rivaled over fabricating an uncharted post-War World II world order. Following the latter’s collapse, the US emerged as the sole superpower, establishing a unipolar world order and securing significant competitive advantages by influencing regional structures in the Atlantic and Asia-Pacific and extending its formidable military presence.⁸ To that end, China started its rise as an uphill battle by challenging the post-Cold War order, advocating for a “fair” and non-hegemonic global governance system.⁹ Evidently, the most prominent common denominator of Beijing’s closest strategic frameworks is not ideology but rather an anti-American sentiment, often sugarcoated as “multilateralism.”

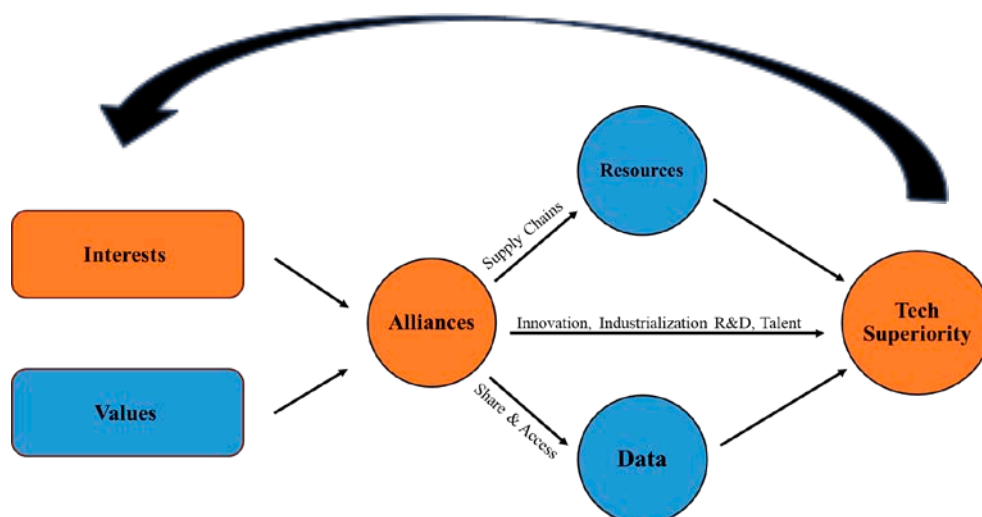
Third, unlike the Cold War, the economic systems of China and the US are deeply intertwined. In 2022, 7.5 percent of total US exports were to China, and 16.5 percent of total US imports were from China.¹⁰ In the same year, the US accounted for 7.2 percent of China’s total imports¹¹ and 17 percent of its exports.¹² In comparison, trade between the US and the Soviet Union accounted for an average of 1 percent of total trade for

both countries throughout the 1970s and 1980s, and mainly consisted of agricultural and basic industrial goods.¹³ The interdependency, the complexity of modern supply chains, and the reliance on specific commodities for advanced technologies have added a new dimension to today's GPC.

The fourth—and arguably the most substantial change between the Cold War era and the current GPC—is the evolving scope and nature of technologies. While technological superiority was a major factor in the US's eventual victory over the Soviet Union, in the “Age of Information” and in conjunction with the Fourth Industrial Revolution, technology now permeates and dominates all aspects of life, assuming the role of ideology as the key lever to influence the balance of power. The ongoing erosion of traditional barriers between civilian and military technologies has transformed national security concepts, extending their reach into societal, political, and cognitive domains. As long as the MAD effect continues to limit the likelihood of a direct military clash between the two major powers, high-end capabilities in cyberspace and the ability to control information flows via social media are far more critical today than modern tanks or deadlier nukes.

Last, the value of data as a strategic commodity is becoming increasingly apparent. In an era dominated by AI and machine learning, the effective collection, usage, and management of data form the backbone of advanced technologies. From military uses such as autonomous systems and social media influence campaigns to civilian applications, including gene sequencing and biomanufacturing, data has become a pivotal element in geopolitical dynamics.

The changes in the building blocks of the modern GPC shifted the essence of power. Alliances today are still formed by shared interests and values, but as long as the competition is not defined and treated as existential, or more precisely, as another Cold War, countries are inclined toward promoting economic, security, and political interests over “choosing sides.” These alliances, in turn, materialize in the formation of supply chains and cooperation on resources, sharing of and access to data, and joint innovation, industrialization, and R&D, all of which accumulate into the ultimate objective of technological superiority: the new indicator of overall national strength. In the current geostrategic framework, technological power is not only the end game in power relations but also the main incentivizer for interest-based alliances, as shown in Figure 2.

Figure 2. The Defining Elements of Great Power Today

In contrast to the Cold War era, where the competition between the US and the Soviet Union was deeply rooted in value-based (ideological) alliances, the current rivalry between the US and China is primarily centered on technological supremacy. Alliances, or in China’s case, “partnerships,” are mainly dominated by interests rather than ideology, leaving an open field for competition over securing resources, strategic infrastructures, and know-how through bilateral agreements, incentives, and coercion. From the US perspective, it is a misuse of its most considerable advantage over its geopolitical rival, rooted in the history of containing the Soviet challenger: value-based alliances in the form of a democratic bloc.

Power-Defining Technologies: A Comparative Analysis

The classifications of technologies considered “critical” or “strategic” are fluid, varying over time and between administrations, and are perceived differently by the US and China. In October 2020, President Trump released the “National Strategy for Critical and Emerging Technologies,” stating that “American dominance in science and technology is more important now than ever, and is vital to our long-term economic and national security.” The strategy outlines the importance of promoting and protecting American leadership in 20 critical technologies, including AI, energy, quantum computing, communications, semiconductors, and space.¹⁴

In February 2022, President Biden’s administration revised the list of Critical and Emerging Technologies (CETs), aligning it with three core national security goals: safeguarding American security, enhancing economic prosperity, and upholding democratic values. Notable updates to the list include the exclusion of agricultural, medical, and public health technologies and the addition of financial technologies, hypersonics, and

renewable energies.¹⁵ Further modifications in February 2024 introduced additional CETs, specifically positioning, navigation, and timing technologies, alongside data privacy, data security, and cybersecurity technologies.¹⁶ The different classifications of CETs are detailed in Appendix A.

China's official papers on emerging technologies are rather scattered and openly address only the economic aspects of CETs. With a stated aim of transforming into a leading global player in manufacturing, China's State Council issued the "Made in China 2025" 10-year national action plan in May 2015. This plan identified 10 priority sectors: new information technology, computerized machines and robots, aerospace equipment, ocean engineering equipment and vessels, rail transportation equipment, energy-saving cars and new energy cars, electrical equipment, farming machines, new materials, and biomedicine.¹⁷

Focusing on industrial policy, China's National Development and Reform Commission (NDRC) issued national guidelines in September 2020 for "promoting high-quality economic development." The plan highlighted eight "Key Industrial Investment Domains": information technology (including 5G, semiconductors, AI, big data, cloud computing, blockchain, and smart infrastructure), biotech, high-end manufacturing, new materials and supply chains, new energy, electrical vehicles (EVs), environmental protection, and digital creative industry.¹⁸

In China's 14th Five-Year Plan (FYP) for the years 2021–2025—the People's Republic of China's (PRC) underlying strategic blueprint for long-term economic and social development objectives—the first action item is dedicated to innovation and self-reliance. The plan prioritizes seven core fields for indigenous R&D that are critical for national security and development: new generation AI, quantum information, integrated circuits, brain science (including "brain-computer fusion"), genetics and biotechnology, clinical medicine and health, and deep space, earth, sea, and polar exploration.¹⁹

A comparison between the US and China's lists of CETs, illustrated in Figure 3, reveals two significant differences. First, genetic editing and synthetic biology are prioritized as the fifth most important field in China's 14th FYP, whereas these fields are absent from US lists. Second, there is an evident difference in the illustration of the strategic value of technological leadership: US policy papers emphasize both economic and national security aspects and include explicit military technologies like hypersonic missiles. In contrast, China's documents primarily present all emerging technologies as drivers of economic growth and development and avoid specific references to military applications.²⁰

Figure 3. CET Lists: Comparative Analysis

Technologies on both lists	Unique to US 2024 list	Unique to China's lists
Advanced computing, new materials, advanced manufacturing, advanced sensing, PNT/satellite technologies, renewable energies, AI, autonomous systems, biotechnology, communication technologies, directed/new energy, human-machine interfaces, quantum information, semiconductors, space technologies and systems	Hypersonics, data privacy, data security and cybersecurity	New energy vehicles; big data; blockchain; bioeconomy; genetic technology; synthetic biology; deep-sea, deep-earth, and polar exploration

The role of CETs in China’s military aspirations of becoming a “world-class armed force”—though not explicitly stated in its official papers on emerging technologies—is evident in President Xi Jinping’s 2015 military reform, which prioritized a technology-driven transformation of the armed forces.²¹ A central mechanism for achieving this goal is China’s Civil-Military Fusion Strategy, which President Xi directly oversees and which aims to integrate the nation’s civilian research and commercial sectors with its military and defense industrial sectors.²² Notably, in its 2015 military strategy white paper, China committed to “accelerating civil-military integration in key sectors” and “establishing uniform military and civilian standards for infrastructure, key technological areas, and major industries.”²³

“In Modern Warfare, Victory Hinges on Information”

With the inevitable erosion of traditional barriers between the civilian and military implications of emerging technologies, a challenge arises in defining which are primarily commercial and which directly impact national security. Nevertheless, the distinction is vital for deciphering the essence of the current GPC and both sides’ underlying interests.

If power was traditionally measured by military might, the emergence of nuclear weapons during the Cold War resulted in a “balance of terror,” which narrowed the role of great power militaries to power projection and conventional proxy wars. While the theory of nuclear deterrence has yet to be refuted, the development of emerging and dual-use technologies prompts a reassessment of the potential effect of new military capabilities on the balance of power.

NATO’s report on science and technology trends for the years 2020–2040 classifies eight interrelated areas as “major strategic disruptors” for military capabilities.²⁴ Of these, five are categorized as “disruptive” and hence are expected to have major, or potentially revolutionary, effects in the next 5–10 years: big data and advanced analytics, AI, autonomy, space technologies, and hypersonic weapon systems. The remaining

three—quantum, bio and human enhancement technologies, and novel materials and manufacturing—are categorized as “emerging.” That is, they are expected to reach maturity within a time frame of 20 years, are not currently widely in use, and their effects on military capabilities are not yet entirely clear.²⁵

The gradual fruition and integration of emerging technologies is transforming warfare twofold. First, it is augmenting traditional lethal capabilities and extending them into new domains such as space and cyberspace. Second, it is spilling over to societal and cognitive realms, hence expanding the impact of military technologies beyond purely combat-related applications. While the first category of transformation is *evolutionary* in nature (even though at an accelerated pace), the second has *revolutionary* potential for changing national security paradigms.

From an evolutionary perspective, modern warfare is a continuation of promoting national security and interests via efficient lethal capabilities. The US Department of Defense (DoD) articulates its enduring mission as safeguarding the nation by both deterring warfare and achieving victory should deterrence not suffice. The fundamental function of technologies in the context of conventional warfare can thus be understood as sustaining a military advantage or, at a minimum, ensuring a competitive military symmetry to deter overt conflict. Notably, in its 2018 national defense strategy, the DoD recognized the diminishment of US military advantage amid a security landscape characterized by rapid technological breakthroughs, cautioning that the failure to update military systems to contemporary standards could culminate “in a Joint Force that has legacy systems irrelevant to the defense of our people.”²⁶

An evidential paradigm shift in combat perception transpired in July 2017, when the chairman of the US Joint Chiefs of Staff introduced “Information” (defined as processed data) as the seventh joint function and a new dimension of conflict, the first change to the joint doctrine in two decades.²⁷ Defense Secretary Mattis then stated that “Information is such a powerful tool that it is recognized as an instrument of national power,” which impacts all military operations at the strategic, operational, and tactical levels.²⁸

In the same year, the Pentagon commenced AI to its operations with the establishment of the Algorithmic Warfare Cross-Functional Team, commonly referred to as “Project Maven,” materializing an evolutionary stage of warfare. Project Maven’s objective was “to turn the enormous volume of data available to DoD into actionable intelligence and insights at speed,”²⁹ ultimately facilitating machines to take over human roles in military detection of objects. The Maven Smart System had since been operational in regions such as Ukraine and the Middle East, analyzing diverse multiple data streams—including satellite imagery, geolocation data, radio systems, heat-detecting infrared sensors, electronic surveillance, and social media feeds—thereby providing military commanders precise intelligence of ongoing developments on the battlefield.³⁰

Concurrently, China’s 2017 AI development plan calls for securing global AI leadership by 2030 and enhancing AI civil-military integration.³¹ In its 2019 national defense

white paper, China introduced the concept of “intelligent warfare,” driven by the applications of AI, quantum information, cloud computing, and the Internet of Things (IoT).³² The People’s Liberation Army (PLA) has since developed a core operational concept titled “Multi-Domain Precision Warfare,” leveraging communications and big data analytics to swiftly identify critical vulnerabilities in US operational systems.³³ Further advancing this strategy, in April 2024 President Xi launched the PLA’s Information Support Force as a new strategic military branch. A *PLA Daily* commentary then stated that network information technology has become the “biggest variable in the development of the times, as in modern warfare, victory hinges on information.”³⁴

Although the tactical use of networked information technologies in combat is developing, it remains evolutionary in nature rather than revolutionary. The use of unmanned aerial vehicles (UAVs) for reconnaissance missions, for example, dates back to World War II, and their employment in combat has been rapidly evolving since operation Desert Storm.³⁵ With advancements in technology and reduced production costs, drones have significantly impacted conventional warfare, notably altering the course of the 40-year military stalemate in Nagorno-Karabakh by overwhelming the outdated Armenian defenses.³⁶ However, the recent war in Ukraine highlights the limitations of such technological leaps, as both Russian and Ukrainian forces have rapidly adapted by innovating, emulating, converting commercial technologies, and developing anti-drone tactics,³⁷ thereby restoring a balance in technological capabilities.

Similarly, hypersonic weapons technologies are largely considered as disruptive, as their speed, precision, and maneuverability are apt to overcoming contemporary missile defense systems, with the potential to nullify the MAD effect by preemptively annihilating nuclear arsenals and second-strike capabilities.³⁸ Nonetheless, the strategic significance of hypersonic weapons remains dubitable as their effect is similar to that of existing intercontinental ballistic capabilities, and for as long as tradition principles of nuclear deterrence hold, it would seem inconceivable to apply them in a direct major-power confrontation.³⁹

As both military and civilian modern technologies increasingly rely on information, communication, speed, and precision, the space domain evolved into a central pillar of national security. In August 2019, President Trump established the US Space Command as the 11th geographic combatant command, designating space as “the next warfighting domain.”⁴⁰ Soon after, the US Space Force was inaugurated as the first new branch of the armed services since 1947, with a stated primary mission of preserving space superiority, an objective characterized by the ability to execute all-domain operations at any designated time and location, free from significant interference by adversarial space or counterspace forces.⁴¹

Modern armies are structured around the premise of having access to space capabilities, including positioning, navigation, surveillance, reconnaissance, early warning systems, and unbounded universal communication. These capabilities are essential for

major powers aiming to sustain a global presence and protect interests and allies around the world,⁴² as evident by the role of US-based Starlink commercial satellite services in supporting Ukraine's fighting capabilities against Russia.⁴³ The buildup of counterspace capabilities—namely electronic warfare, cyberattacks, and anti-satellite missile—is therefore considered a strategic threat that can impede not only combat readiness but also space-enabled civilian services, including communications, aviation, critical infrastructure, and international trade.⁴⁴ From the US perspective, the destruction of satellites in the pursuit of military objectives is considered an act of war.⁴⁵

Essentially, achieving superiority in lethal military capabilities can potentially influence the balance of power on three levels: a full-scale or limited direct clash between the great powers, a strategic military action involving one of the powers, or through proxies. Nevertheless, as long as military capabilities remain evolutionary in nature and advance in a more or less symmetrical parallel, a direct full-scale showdown between the powers would still be subject to traditional deterrence principles and can therefore be considered implausible at this point. While limited direct confrontations can emerge in forms of power projection, for example, by defending allied countries and interests, or erupt unintentionally due to miscalculations or misperceptions, these would unlikely escalate to a direct full-scale US-China war.

A strategic military action by one of the powers could affect the balance of power by strengthening, weakening, and turning alliances (and in consequence, access to resources, supply chains, and data), or by seizing advanced technologies by force. US Commerce Secretary Gina Raimondo addressed such a scenario, stating that a Chinese invasion of Taiwan and the capture of world-leading chip producer TSMC would have a devastating effect for the American economy, which acquires 92 percent of its leading chips from the company.⁴⁶

On the proxy level, lethal military applications can change the balance of power by feeding into interest-based alliances. While evolutionary warfare tools such as hypersonic missiles and UAVs are not likely to be dispatched between the great powers, their deployment could significantly alter the dynamics of smaller-scale conflicts by providing one party with an asymmetrical advantage, as evidenced in the Nagorno-Karabakh conflict. Furthermore, these military innovations may function as inducements to advance political and economic objectives, exemplified by media reports on the importance of advanced US weapons in facilitating the Abraham Accords.⁴⁷

TikTok, Encryption, and Human Cognition: New Technological Battlefields

A major revolution in national security concept is the spillover of warfare to nonkinetic domains, with the capacity of influencing societies, political stability, and human cognition. The DoD anticipates a substantial escalation over the next two decades in activities

characterized as “gray area” operations, as they are understood to fall below the conventional threshold for military action. Such operations, which include malign cyber and space operations, economic coercion, and disinformation campaigns, are growing in sophistication and create new challenges for defensive enterprises.⁴⁸

As global society progresses into an era of increased digital dependency and interconnectivity, critical infrastructures, space-enabled services, and routine online activities are ever more vulnerable to cyber warfare’s disruptive impacts.⁴⁹ Incidents such as the 2007 Russia-based cyberattacks on Estonia, which crippled essential online services such as banking, news, and email communications for three weeks,⁵⁰ and the 2021 Colonial Pipeline ransomware attacks, serve as stark illustrations of the potential to impair a country’s national and economic security via nonkinetic warfare. Even if the operational successes of such attacks are limited, they can still carry significant psychological effects and undermine the general public’s sense of security.

In its 2023 National Cybersecurity Strategy, the DoD assessed that in the event of a direct conflict, China will likely launch destructive cyberattacks against the US with the aim of impairing military capabilities, sowing chaos, and diverting attention and resources. It further recognized China as a “broad and pervasive cyber espionage threat” that surveils individuals beyond its borders and steals technology secrets in an effort to erode US military advantage. Additionally, the strategy raised concerns about China’s ambitions to propagate digital authoritarianism around the globe by exporting its own cyber capabilities to like-minded nations.⁵¹

Similar allegations are raised by China against the US. An April 2024 report composed by a group affiliated with Cyberspace Administration of China accused the US of both abusing cyberspace for maintaining its hegemony and triggering a “cyber arms race” as a main battlefield of a new Cold War. The report highlights findings from the Snowden leaks and WikiLeaks of US covert data collection and global espionage, and concludes that the US normalizes the use of cyberattacks to advance its military, economic, and diplomatic interests under the justification of national defense.⁵²

Another revolution in national security concepts arises from the vast quantities of personal data, generated and harvested both from direct digital interactions and indirectly through smart devices, and the new avenues for exploitation, surveillance, manipulation, and extortion.⁵³ The *New York Times*’s 2019 Privacy Project exemplifies how accessible, vulnerable, and susceptible personal data is, as information that is being collected daily by commercial actors is often resold to third parties. In fact, any owner of a mobile phone is likely tracked by dozens of companies, often by consent to location sharing for various apps. By obtaining access to such a dataset, the journalists were able to identify a location ping of a security detail in President Trump’s entourage and then track down the president’s precise location throughout the day.⁵⁴

Leaks and theft of personal data pose a new dimension of threat. Notably, in 2015, two major breaches of US government databases, which were attributed to the Chinese

government, exposed sensitive information on more than 22 million citizens, including federal employees, contractors, and their families. Regarded as one of the most potentially damaging cyber heists in US government history, the stolen data included not only personal identifiers and addresses but also extensive financial and health records, fingerprints, and digital credentials such as usernames and passwords. The exposure of such information is particularly alarming due to its potential use in compromising US intelligent operatives, or to identify government employees who might be susceptible to extortion and coerced to engage in espionage.⁵⁵

The value of personal datasets extends beyond immediate time and traditional military- and security-related espionage targets. As information on everyday citizens is collected in mass and stored in clouds, it can also be extracted in the future, in the event they assume positions of interest or affiliations with people of interest. Accordingly, foreign governments may leverage details on indebtedness, medical conditions, and other embarrassing personal information to coerce employees within strategic sectors into disclosing sensitive information, obtain crucial technological insights from scientists, undermine election campaigns, and influence politicians.⁵⁶

Democratic elections serve as fertile grounds for such influence campaigns. The US Intelligence Community's annual threat assessment specifically identified a risk of Chinese attempts to manipulate the 2024 elections to support its goals and interests by magnifying societal divisions, disseminating disinformation, and sowing doubts about US leadership. According to the report, China's propaganda arm had already used TikTok accounts to target candidates from both political parties during the 2022 US midterm elections, and has since escalated its sophistication in influence activities by adopting generative AI technologies.⁵⁷

The DoD's 2023 annual report on China's military and security developments attributes the aforementioned activities to a wider paradigm of PLA-led influence operations, in which Chinese narratives are promoted internationally via social media platforms. The report identifies the PLA's Strategic Support Force (SSF)—a theater command-level organization centralizing its capabilities on space, cyberspace, information, and communications—as the military branch in charge of developing the next evolution of psychological warfare, dubbed Cognitive Domain Operations (CDOs).⁵⁸ Incorporating AI, big data, and neuroscience technologies, CDOs are claimed to aim at subverting human cognition and behavior beyond the realms of the battlefield, shaping and polarizing societies, and creating an environment favorable to China.⁵⁹

FBI Director Christopher Wray described related national security concerns in TikTok's operations, as the company “is beholden to the Chinese government” and therefore might provide Chinese intelligence services three powerful tools: the ability to collect US citizens' personal data and use it for influence operations, to control recommendation algorithms and push narratives of the Chinese Communist Party (CCP), and to manipulate the software and potentially compromise users' devices.⁶⁰ The concerns from the

US Intelligence Community correspond with TikTok's rapid growth in the country, not only in unique users but also in influence. According to a 2023 Pew Research Center poll, 14 percent of US adults regularly consume their news from TikTok. The number is significantly higher among younger populations, amounting to 32 percent between the ages of 18 and 29.⁶¹

A source for suspicion regarding the relationship between Chinese companies and the CCP is the nation's 2017 National Intelligence Law, which mandates Chinese companies to "support, assist, and cooperate with" its intelligence-gathering authorities. Such concerns have been directed toward Huawei, the world's foremost provider of 5G networks and a leading seller of telecommunications equipment.⁶² With the global dependence on 5G infrastructure expected to increase significantly, security experts warn that Huawei could be forced to embed backdoors in the hardware or software, allowing Beijing remote access to all circulated data in the network and the possibility to interfere with communication services in the event of conflict.⁶³

As the value of data and information control emerges as a defining pillar of national security, both great powers have been taking protective measures to protect it. In May 2019, President Trump signed an executive order to secure US information and communications technologies, laying the groundwork for the Federal Communications Commission's (FCC) designation of Huawei as a national security threat in June 2020.⁶⁴ In February 2024, President Biden issued an executive order to protect Americans' sensitive personal data from exploitation "by countries of concern," directing the issuance of regulations and high security standards to safeguard sensitive genomic, biometric, health, geolocation, and financial data.⁶⁵ By April 2024, further actions were taken as President Biden signed legislation requiring ByteDance, the parent company of TikTok, to divest the platform within 270 days as a precondition for its continued operations in the US.⁶⁶

In contrast, China has maintained stringent controls over access to mainstream Western social media platforms since 2009,⁶⁷ as it accuses the US of using the internet as a subversion instrument for advocating democratic norms around the world.⁶⁸ Recent years have seen an intensification in the governance and control of data within China, marked by the enactment of three pivotal laws. The 2017 Cybersecurity Law restricts the access of foreign IT and requires foreign companies to store their data in China and share it with local security agencies. Enacted in September 2021, the Data Security Law imposes governmental oversight over all companies and the majority of data-related activities in the country, effectively limiting the overseas transfer of sensitive data. Furthermore, the November 2021 Personal Information Protection Law regulates the collection, application, and monitoring of personal information.⁶⁹

Despite ongoing efforts to secure data and enhance encryption methods, the rapidly advancing field of quantum information science (QIS) may soon render these measures obsolete. Though still in nascent stages of operations, it is a matter of time until

a quantum computer will reach sufficient size and sophistication to be able to break all existing methods of encryption,⁷⁰ in what has been commonly referred to as “Q-day.” While the full range of applications of quantum computers is still unknown, their transformative impact on national security is widely acknowledged, as the political power to harness this technology first will possess unprecedented capabilities, including the ability to decrypt military intelligence, acquire intellectual property, and access vast quantities of digitally stored personal data.⁷¹ The economic and technological implications of quantum computing are addressed in the following section.

In the context of the GPC, national security paradigms are witnessing a substantial revolution, in which the impact of digital “gray area” operations gradually exceeds traditional physical applications. In an era of global digital dependency and interconnectivity, nonkinetic offensive capabilities transcend military targets and extend their reach into societal, political, and cognitive domains, posing significant challenges for national defense. However, while technological advancements in AI, quantum computing, data control, and cybersecurity are critical in establishing military dominance, their broader commercial uses and potential to drive societal transformations hold even greater significance in shaping the global balance of power.

Makers, Takers, and Laggards: A First-Mover Race to Reshaping Societies and Economies

Technological superiority was already an imperative element of the Cold War and its outcome. While the root causes of the Soviet Union’s decline were economic failures and a loss of faith in the communist ideology, its systematic inability to adapt to significant technological changes expedited its collapse. The Third Industrial Revolution, also known as the Age of Information, shifted the traditional economic system via digitization, automation, and the widespread use of personal computers. However, in a reality of intensified globalization in which information had become a critical commodity, the tightly controlled Soviet system struggled to restructure its industries. According to some estimations, by the end of the 1980s, only 8 percent of the Soviet industry was globally competitive, and in the words of Joseph S. Nye, “it is difficult for a country to remain a superpower when the world doesn’t want 92 percent of what it produces.”⁷²

Similar principles now hold as the rapid pace of technological innovation continues to transform the global economic landscape and societal structures. The Fourth Industrial Revolution extends the digital advancements of its predecessor by merging physical, digital, and biological spheres, and facilitating unprecedented levels of interconnectivity among individuals, devices, various industry sectors, and distinct aspects of life.⁷³

The designation of emerging technologies as “critical” primarily reflects their role in facilitating this interconnected global landscape. However, most of these technologies serve specific purposes or act as enablers for other applications. For instance,

semiconductors are integral to the operation of nearly all advanced technologies, yet their standalone value is limited. Additionally, advancements in materials science may lead to new technologies that could supplant the current role of semiconductors. Among the array of emerging technologies, two stand out as general purpose, possessing the transformative potential to reshape entire economies and societies: AI and biotechnology.

AI is widely perceived as the backbone of future defining technologies with the capacity of revolutionizing human potential and addressing societal challenges. In its 2021 final report to the president and Congress, the National Security Commission on Artificial Intelligence (NSCAI) equated the future impact of AI on humanity to that of electricity, “transforming many aspects of human life and every field of science.” Rather than an end-use technology, the report illuminates that “AI sits at the center of the constellation of emerging technologies,” enabling some, such as biotechnology, and being enabled by others, such as 5G communication and quantum computing.⁷⁴

Among the fields in which AI is projected to supercharge key scientific breakthroughs are material and life sciences. The discovery, design, and application of nanomaterials, biopolymers, quantum, and thermoelectric materials are poised to transform economies, public health, and national defense and to facilitate the transition to an energy-efficient, low-carbon economy. In the domain of life sciences, the synergistic integration of AI, biotechnology, and big data is set to revolutionize our understanding and capability to manipulate biological processes at various levels—from the molecular to the ecosystem scale, with tremendous implications for the future of agriculture, food security, personal health, and longevity.⁷⁵

The AI-driven economy already impacts nearly 40 percent of current global employment⁷⁶ and is set to further grow in size and impact. According to a 2023 McKinsey & Company report, the annual economic value of nongenerative AI and analytics is estimated at \$11–\$17.7 trillion, materialized mainly by optimizing performance and problem-solving across industries and business functions. The era of generative AI, while still in its first stages, is projected to add the equivalent of \$2.6–\$4.4 trillion annually, primarily in the areas of customer operations, marketing and sales, software engineering, and R&D. The report notes that the potential economic value of generative AI may even double, as technologies that are embedded into existing software could be used for other tasks. To put this into perspective, the United Kingdom’s entire GDP in 2021 was \$3.1 trillion.⁷⁷

In the looming age of AI, and with the race for technological supremacy at the core of the current GPC, first movers benefit from accelerated development, access to markets, and global standard settings. Based on the assumption that AI would reshape industries and societies, the leader in this race would also be in a favored position to redefine the global economic architecture of makers, takers, and laggards.

However, achieving a leadership position in AI entails mastering several critical components. Professor Ben Buchanan, special advisor on AI to the White House, previously

identified the three drivers of modern AI as algorithms, data, and computing power. In this triad, the quality of a machine learning system is a factor of the talent that programs the algorithms, the quantity and salience of the gathered data, and the computing power needed to process datasets and allow systems to learn on their own.⁷⁸

Alongside the technological dimensions of the competition, the capacity to dominate and enhance AI performance is significantly influenced by national policies and practices. In the realms of algorithms and software, the primary battleground is the development of sophisticated deep-learning generative AI programs, such as large language models (LLMs) that possess the capability to convincingly execute prompts and produce text, images, audio, and videos. However, as these programs increasingly improve in mimicking human behavior, trade-offs emerge between the rapid pace of innovation and the need for effective governance.⁷⁹

In the US, the pursuit of AI leadership is spearheaded by private-sector tech companies currently operating within largely unrestricting policy frameworks. While this environment facilitates swift progress, it also raises substantial risks, including increased susceptibility to issues like deepfakes, manipulation, and the spread of disinformation. Conversely, in China, the internet and associated technologies are subject to stringent governmental controls. In a notable move, in July 2023 the Cyberspace Administration of China implemented regulations that mandate the labeling of all AI-generated content and impose punitive measures on generative AI services that fail to adhere to the state's "core socialist values."⁸⁰ While such measures may enhance control over the technology and potentially prevent abuses, they are also likely to hinder technological progress, both by limiting the availability of generative AI's training data⁸¹ and discouraging tech companies and entrepreneurs who may fear the repercussions of noncompliance.⁸²

As for the data that underpins AI, China's top-down approach and tightly regulated technology sectors confer a distinct advantage. While Western governments operate under stringent privacy constraints vis-à-vis the public and the companies that collect the data, private enterprises in China are mandated to share users' personal data with government authorities.⁸³ Additionally, the state employs an extensive array of surveillance technologies—including numerous cameras with facial and auditory recognition technology, the collection of DNA samples, and tracking devices embedded in mobile phones—to link individuals' digital interactions with their physical movements.⁸⁴ Further enhancing its data control, China inaugurated the National Data Administration in October 2023 to coordinate the integration, sharing, and application of data resources as well as to advance its digital economy and AI industrial development.⁸⁵

In line with the advancements and the widespread use of AI technologies and applications, and as the technological basis enabling AI growth, the demand for computational power and more capable semiconductors rises.⁸⁶ Defined by the White House as "the technology that forms the foundation of everything from automobiles to household appliances to defense systems,"⁸⁷ the semiconductor industry is among the most critical

sectors of the global economy, generating over half a trillion dollars in sales in 2022 alone and enabling economic activity valued at tens of trillions of dollars annually.⁸⁸

The sophistication of advanced semiconductors, exemplified by Nvidia's 4 nanometer chip, which houses 208 billion transistors,⁸⁹ embodies a culmination of numerous technological breakthroughs. The intricate production process of these semiconductors, which encompasses over 500 distinct steps from specialized design software to fabrication plants and testing facilities, renders it infeasible for any single company or country to monopolize the global supply chain.⁹⁰ Consequently, acquiring leadership in AI-enabling hardware such as microprocessors, quantum computing systems, and essential raw materials heavily relies on the effective deployment of alliances, power projection, and influence over the global supply chain.

To enhance US competitiveness in semiconductor technologies, the Biden administration adopted a dual strategy. This involved invigorating domestic production through the allocation of \$280 billion to the CHIPS and Science Act in August 2022 while simultaneously imposing a series of unilateral export control measures on China starting in October of the same year. Jake Sullivan, US national security advisor, then asserted that the restrictions were "premised on straightforward national security concerns" as an implementation of the "small yard, high fence" concept to protect critical technologies.⁹¹

With the objective of reinforcing US leadership in the semiconductor industry and ensuring compliance with sanctions, the US has capitalized on its strategic advantage over its geopolitical rival—its alliances—to establish an ad hoc technological bloc. Under significant diplomatic pressure, the Netherlands and Japan, both critical members of the global semiconductor supply chain and producers of some of the most sophisticated manufacturing equipment, aligned with the US policy by similarly restricting their exports to China.⁹² In a further demonstration of US diplomatic potency, February 2023 saw the establishment of the "Chip 4" alliance between the US, Japan, South Korea, and Taiwan, home to the world's leading chipmakers and suppliers of relevant materials and equipment, to ensure the stable supply of semiconductors.⁹³

While the US consistently frames national security as justification for imposing technological export restrictions on China, Chinese officials contend that the underlying goal is to pursue US hegemony by means of economic coercion and promoting deglobalization.⁹⁴ In response to these restrictions, China leveraged its strategic control over the global supply chain of rare earth metals, crucial components in almost every technological application including smartphones, EVs, wind turbines, and military hardware.⁹⁵ In August 2023, China initiated measures to restrict its gallium and germanium exports to the US, both vital materials for semiconductor manufacturing. This was followed by a further restriction in October 2023 when China limited exports of graphite, an important element in the production of EV batteries.⁹⁶

Despite the efforts to hinder China's semiconductor industry, in August 2023 Huawei introduced its new Mate 60 Pro smartphone, powered by 7 nanometer chipsets

developed in-house. While still two generations behind Apple's 3 nanometer chips, a technological gap estimated at five years,⁹⁷ it is still overall competitive with the iPhone 15⁹⁸ and serves as testament for China's resourcefulness. Eventually, the critical significance of new generational chips is not in improving performance of communication devices⁹⁹ nor in the gradual enhancement of existing military applications. Instead, their fundamental value lies in empowering the capacity of high-performance computing (HPC) and AI to accelerate scientific discoveries, transform industries, and tackle global challenges.¹⁰⁰

For the time being, the development of AI is still progressing at a relatively symmetrical pace as both the US and China possess competitive strengths and weaknesses. But the race for AI superiority does have an endgame, at least in theory, with the possible emergence of artificial general intelligence (AGI). Dubbed as the "Holy Grail" of AI, the vision of AGI is of a system that equals or exceeds human cognitive abilities and can autonomously solve complex scientific issues, including enhancing its own functionalities through self-learning across multiple data domains. Former Google CEO Eric Schmidt projected that the country that first achieves AGI could secure an era of predominance by gaining an edge in all domains of science and technology.¹⁰¹ While estimations of when such level of superintelligent system will arrive vary, the competition is already heated in the US, with companies such as OpenAI, Google DeepMind, and Meta explicitly stating that reaching AGI is their ultimate goal.¹⁰²

In parallel with the AI race, both China and the US are galloping toward solidifying their position in the QSI value chain. In addition to their military potential application of breaking encryption, quantum technologies are poised to supercharge the Fourth Industrial Revolution by redefining the scale and boundaries of computing power.¹⁰³

In classical computing, increasing processing power is achieved by fitting more transistors onto a single chip. However, as modern microchips already squeeze in hundreds of billion transistors, it is an increasingly costly and complex endeavor, which, according to industry experts, is close to reaching its feasible limit.¹⁰⁴ While conventional transistors store bits (binary information units of either a zero or a one), the quantum version of the bit, known as qubit, theoretically has an infinite number of possible states, thus exponentially multiplying the computational power and speed of computing chips.¹⁰⁵

Although advances in quantum computing have been gradual, major technology companies in both the US and China are actively developing and using quantum processors. A Boston Consulting Group (BCG) forecast suggests that maintaining the current rate of technological advancement, quantum computing could begin to deliver business value by 2025, with potential revenue generation estimated between \$450 and \$850 billion upon reaching technological maturity in 2035.¹⁰⁶ Furthermore, a McKinsey analysis projects that quantum computing could unlock economic value up to \$2 trillion by the same year, with the finance, chemicals, pharmaceuticals, and automotive industries expected to be the primary beneficiaries.¹⁰⁷

Quantum technologies are of strategic economic importance within the framework of GPC, as early adopters are anticipated to capture up to 90 percent of the resultant economic value,¹⁰⁸ develop governance models, ensure global interoperability, and catalyze more scientific breakthroughs.¹⁰⁹ The transformative role of quantum in the pursuit of technological supremacy is evident in China's 14th FYP, ranked second in its science and technology priority list.¹¹⁰ In terms of government investments, Beijing has so far publicly announced \$15.3 billion in quantum R&D and education, starkly surpassing the \$3.8 billion committed by the US. However, the trend is reversed in terms of private financing, with the US totaling \$3.8 billion in private investments, more than tenfold in comparison to China's \$360 million,¹¹¹ underscoring the contrasting approaches between China's state-led strategy versus the US company-driven innovation.

Biopower: Hacking Life, Fostering Discoveries, and Shaping Generations

Alongside AI, biotechnology stands as a pivotal, general-purpose field of technology at the core of the GPC. Traditionally associated with pharmaceuticals and agricultural products, recent innovations in synthetic biology have brought the sector to the brink of a transformative revolution, enabling the engineering of biological systems at the DNA level. From precision medicine and human enhancement to enriched foods, disease-resistant crops, clean energy production, and the creation of novel materials, the implications of the emerging biotech era extend across economic, security, and ethical domains.¹¹²

From an economic standpoint, the innovative use of biological resources and processes is catalyzing the growth of the bioeconomy—a burgeoning sector increasingly influential across various industries.¹¹³ According to a McKinsey report, as much as 60 percent of global physical inputs could potentially be produced biologically. The report estimates the direct annual global impact of the bio-revolution at between \$2 and \$4 trillion in the years 2030–2040,¹¹⁴ while a separate BCG study evaluates the broader economic effect at up to \$30 trillion globally over the next decade.¹¹⁵ The defining influence of the emerging bioeconomy on the balance of power has been underscored by the US Intelligence's 2024 Annual Threat Assessment, stating that the country that will lead biotechnological breakthroughs will not only hold trillions of dollars in production capacity and drive industry growth but also wield substantial influence over the global economy for generations.¹¹⁶

Apart from the direct economic implications, biotechnologies play a central role in the US “derisking” strategy, which aims to reduce critical dependencies on China by encouraging self-sufficiency and the formation of resilient supply chains.¹¹⁷ In September 2022, a few weeks after signing the CHIPS and Science, the Biden administration issued the executive order on “Advancing Biotechnology and Biomanufacturing Innovation.”

Among its stated goals, this order aims to replace fragile supply chains from abroad with domestic production, highlighting that the US reliance on foreign materials jeopardizes its access to vital chemicals and active pharmaceutical ingredients.¹¹⁸

In March 2023, only six months after the executive order, the White House released a new report, *Bold Goals for US Biotechnology and Biomanufacturing*, prioritizing five societal goals for the next two decades: climate change solutions, food and agricultural innovation, supply chain resilience, human health, and cross-cutting advances. Addressing critical supply chain vulnerabilities, the report sets a goal of harnessing biomanufacturing to produce 25 percent of domestic demand in active pharmaceutical ingredients in the next 5 years and at least 30 percent of the US chemical demand within a time frame of 20 years.¹¹⁹

The report identifies “cross-cutting advances” as essential components for fostering new discoveries that will propel advancements across all sectors of the bioeconomy. This begins with the mapping and research of genes in newly discovered species to elucidate their potential physical traits. Given the vast and largely unexplored biodiversity on Earth, which includes millions of species of plants, animals, and fungi, as well as approximately one trillion species of microbes, the pool of knowledge that can be applied in novel biotechnologies is immeasurable. The plan aims to sequence the genomes of one million species within the next five years and, by leveraging innovations in computing power and AI, to accelerate the discovery of new gene sequences, metabolisms, and functions by 100-fold within a span of 20 years.¹²⁰

While the US is ramping up its attention to the strategic value of synthetic biology, China’s ambition to dominate the field goes back to 2010, when it identified biotechnology as one of seven strategic emerging industries essential for its economic competitiveness. Subsequently, biotechnology was already integrated into China’s 12th FYP (2010–2015), which aimed at establishing a national gene resource library and advancing biomanufacturing, genetic engineering, and digital medicine. The 13th FYP (2016–2020) continued this trajectory, expanding the application of genomics and biotechnologies in medicine and creating Chinese gene and cell banks.¹²¹ In its 14th FYP (2021–2025), genetics and synthetic biology were ranked fifth on the science and technology priority list, emphasizing innovations in genetic cells and genetic breeding.¹²²

Among the various applications of biotechnology, China has placed significant emphasis on the field of biomedicine. Recognized as a priority sector in the “Made in China 2025” strategy, the plan sets goals to attain world-class standards in innovation capacity, production volume, and international competitiveness in the pharmaceutical sector by 2025.¹²³ Correspondingly, in 2016, the PRC launched a \$9 billion project aimed at collecting, analyzing, and sequencing genomic data over a period of 15 years to position itself as a global leader in precision medicine.¹²⁴

For more than a decade, China’s concerted efforts to gather extensive amounts of biological data globally, including acquisitions of US genetic-sequencing firms,

proceeded largely unimpeded. However, as general awareness of the strategic importance of personal data increased, concerns emerged over the potential misuse of such data, particularly due to the operating company of the China National GeneBank—the PLA-affiliated BGI Group.¹²⁵ Accused of exploiting DNA for the genetic surveillance of Muslim minorities in Xinjiang, the US Department of Commerce sanctioned two subsidiaries of BGI in July 2020,¹²⁶ followed by another two of its holdings in March 2023, citing risks of using genetic data to support Chinese military programs.¹²⁷ Other allegations against the company included the covert swiping of DNA from its massive global distribution of COVID-19 test kits and commercial parental tests.¹²⁸

From a national security perspective, stakeholders and US government officials admit that it is challenging to fully comprehend the threats that may emerge from leveraging genetic data.¹²⁹ At the far end of the threat spectrum, there are concerns about the development of targeted biological weapons that could be deployed against individuals, populations, or agricultural resources. More frequently discussed are issues related to data security, with claims that sensitive genetic information could also be exploited for espionage purposes or to extort vulnerable individuals. Bill Evanina, former director of the US National Counterintelligence and Security Center, has long voiced concerns regarding China’s alleged intentions, noting that “from a biotech perspective BGI is no different than Huawei,” in the sense of a “legitimate business that’s also masking intelligence gathering for nefarious purposes.”¹³⁰

In response to growing concerns about the security and commercial ramifications of failing to match China’s advancements in biotechnology, in January 2024 US legislators introduced a bipartisan bill referred to as the “Biosecure Act.” This legislative proposal aimed to limit cooperation with “biotechnology companies of concern,” naming four Chinese biotechnology firms and their subsidiaries, including BGI. Mike Gallagher, then chair of the House Select Committee on the CCP and sponsor of the House version of the bill, highlighted the ethical implications of leadership in biotechnology, stating that “the country who wins the race will set the ethical standards around how these technologies are used.”¹³¹

One of the most contentious ethical issues within biotechnology pertains to the use of genetic advancements for enhancing human performance, capabilities, and health. Within the GPC framework, the mastery over technologies that could enable longevity, immunity from diseases, or heightened cognition holds significance comparable to the dominance of AGI. However, unlike AGI, human enhancement technologies have already manifested, as shown by the notorious 2018 incident involving Chinese biophysicist Dr. He Jiankui, who used CRISPR technology to genetically modify twin girls to be resistant to HIV.¹³²

While human genome editing is prohibited in at least 70 countries, including China and the US,¹³³ this affair highlights the precarious nature of technological proliferation. Should the alteration of human genetics become a competitive arena, with the very

essence of humanity as we know it at stake, principles of game theory suggest that the drive to avoid strategic disadvantages may set off a human-enhancement arms race.

One World, Two Systems: The Inevitable Path to Technological Decoupling

A strategic benefit for early adopters in the quest for technological dominance lies in their ability to establish international norms and technical standards. In a globally connected environment, these standards ensure compatibility, interoperability, and efficiency, enabling consistent use of physical and digital technologies across different countries.¹³⁴ For the US, decades of dominance in standards development have been instrumental to its global technological leadership and economic prosperity, as its private sector effectively set the rules that govern today's global communications and internet protocols.¹³⁵ Furthermore, the establishment of standards and issuance of patents can generate substantial economic benefits. For instance, Qualcomm reported over \$7 billion in licensing revenues in 2022 alone, primarily from granting rights to use its intellectual property in the manufacturing and sales of wireless products.¹³⁶

Until recently, the process of setting technical standards was perceived as a nonpolitical endeavor. International standards developing organizations (SDOs), comprised of academics, civil society, engineers, and industry experts, traditionally select commercial proposals for technical solutions based on criteria like safety, efficiency, and interoperability. While SDO decisions are voluntary and nonbinding, they hold profound strategic and economic significance,¹³⁷ affecting approximately 93 percent of worldwide goods exports.¹³⁸ Consequently, companies unable to establish their technical standards often incur royalty payments for patent use and may need to redesign products to align with recognized international standards.¹³⁹

From a security standpoint, some experts contend that developers of internationally standardized technologies often possess detailed knowledge of their vulnerabilities, a consideration of critical importance regarding digital infrastructure. Moreover, next-generation technologies associated with the Fourth Industrial Revolution entail political and ethical dimensions as their algorithmic design is bound to comply with certain norms, values, and regulations in issues such as data privacy standards. As emerging technologies increasingly permeate and integrate into all facets of life, the capacity to define international standards carries tremendous weight in molding the industries of the future and, consequentially, the global balance of power.¹⁴⁰

In an effort to better its position in the uphill battle against US dominance in setting international standards, China introduced its "Standards 2035" strategy in March 2018, aiming to set the rules of global production across key industries.¹⁴¹ The specifics of this strategy were further detailed in the "National Standardization Development Outline" published in October 2021, which underscored the prioritization of standardization

initiatives in the fields of AI, quantum information, and biotechnology, with an overarching objective to incorporate Chinese standards into the development of general-purpose technology platforms.¹⁴²

To achieve these objectives, China has implemented a dual strategy. Within multilateral settings, it expanded its presence in strategic SDOs like the International Telecommunication Union, gained more influence over the agenda, and compelled Chinese companies to align their votes, often prioritizing national interests over technical merits.¹⁴³ According to some testimonies, Chinese delegates were occasionally required to verify their compliance by showing proof of their votes on their mobile devices. Simultaneously, China has been actively setting “facts on the ground” by pushing its standards through bilateral agreements and the Belt and Road Initiative. This approach effectively establishes long-term dependencies in host countries, as once infrastructures like 3G/4G communication networks powered by Chinese technology are in place, high costs of transitioning to other standards lock these nations into China’s technological ecosystem.¹⁴⁴

As the adoption of standards increasingly incorporates geopolitical considerations alongside technical merits, the potential for a split into two distinct technological ecosystems grows more pronounced. Technological decoupling is by no means a hypothetical scenario, as evident by the great power clash in the global rollout of 5G communication networks. The US, citing security reasons, has vigorously campaigned against the deployment of Huawei’s top-of-the-line and cost-effective 5G solutions, leading to a bifurcation in global communications infrastructure. Similarly, given the existing bans on Western social media platforms and numerous traditional news outlets within China, it seems implausible that technologies involving Western-developed generative AI algorithms would be adopted there, regardless of their international recognition.

The global effort to develop a COVID-19 vaccine illustrates the division into a “one world, two systems” reality. Using AI, US companies like Pfizer and Moderna rapidly synthesized effective mRNA vaccines by analyzing millions of data points. In contrast, China has opted not to approve these or any foreign vaccines, relying instead on domestically produced inactivated pathogen vaccines, which have shown lower efficacy rates.¹⁴⁵ Its refusal to import US-made vaccines, even during peak outbreaks and national lockdowns,¹⁴⁶ is often attributed by US officials to national pride.¹⁴⁷ Correspondingly, while the World Health Organization granted emergency use authorization to the Sinopharm and Sinovac vaccines in June 2021,¹⁴⁸ they were not approved by the US Food and Drug Administration.¹⁴⁹

One possible reason for the COVID-19 vaccine decoupling is commercial. By mid-2023, Pfizer and Moderna had amassed over \$117 billion in vaccine revenues,¹⁵⁰ whereas China’s export of nearly two billion doses yielded undisclosed revenues.¹⁵¹ Another argument is of global prestige. Josep Borrell, the European Union’s high representative for foreign affairs and security policy, critiqued China and Russia for using “vaccine diplomacy” to extend their global influence by flaunting their contributions, in

discrepancy with the lower efficacy of their vaccines and smaller proportion of donations compared to commercial sales.¹⁵²

Currently, the segmentation of technologies into dual systems remains limited and interoperable. However, as technologies evolve and incorporate more data domains, maintaining compatibility is becoming increasingly complex. EVs serve as a prime example. These advanced “computers on wheels” are equipped with sensors and cameras, which receive and transmit information via satellite connections. For that reason, they are also considered to be a security threat. In China, Tesla’s access to certain government-related areas and districts have been restricted since 2022 due to concerns of compromising confidential information.¹⁵³ Moreover, in February 2024, the Biden administration announced plans to undertake “unprecedented action to address the security risks” associated with Chinese connected vehicles,¹⁵⁴ which, according to Commerce Secretary Raimondo, might culminate in a total import ban on such vehicles.¹⁵⁵

At the micro level, the vulnerabilities associated with EVs extend to virtually all connected devices. Modern electronic devices, ranging from smartphones and televisions to robotic vacuum cleaners and pacemakers, are capable of recording information and transmitting data and are susceptible to hacking risks. At the macro level, the divergence in AI-enabled technologies, characterized by algorithms embedded with competing values, operating on different internet protocols, and processing distinct datasets, leads to inherent non-interoperability. In a world of two systems, third countries would eventually be compelled to “choose sides” by aligning with specific technological standards and security protocols, thereby shaping the new paradigm of power, with technological blocs at its core.

Conclusion

In the context of the current GPC, technology is the new ideology in terms of the critical determinant of comprehensive strength. As we navigate through the dawn of AI and the biotechnology revolution, transformative scientific advancements are rapidly reshaping global economies, industries, military capabilities, and the fundamental nature of human existence. In this landscape, first movers have the potential to dominate markets, establish international standards, and wield significant economic and political influence that could last for generations.

Achieving technological leadership requires mastering three primary components: hardware, software, and data. In a globalized setting, the success of this endeavor largely hinges on the capacity of great powers to forge effective alliances, which manifest through cooperation across supply chains, resource sharing, innovation, talent acquisition, and data pooling. In the shorter term, technological supremacy also acts as a catalyst for forming interest-driven alliances as third countries aim to advance their national economic, security, and political agendas.

History shows that GPCs rarely end in a decisive outcome; rather, it is a long-term struggle over spheres of influence. Such is the case in the present bipolar rivalry, as the world is increasingly polarizing into two distinct technological ecosystems, each characterized by unique values, standards, and platforms. Although these systems can still, for the time being, correspond, the escalation in bilateral sanctions and restrictions on competing infrastructures and connected devices is propelling the world toward an apparently inevitable division—a new global architecture delineated by two incompatible technological blocs.

Appendix A: CETs Classifications in the US and China

October 2020 US CET List	February 2022 US CET List	February 2024 US CET List	China CET List*
Advanced computing	Advanced computing	Advanced computing	Cloud computing
Advanced conventional weapons technologies	Hypersonics	Hypersonics	
Advanced engineering materials	Advanced engineering materials	Advanced engineering materials	New materials
Advanced manufacturing	Advanced manufacturing	Advanced manufacturing	High-end equipment manufacturing
Advanced sensing	Advanced networked sensing, signature management	Advanced networked sensing, signature management	Smart infrastructure
Aero-engine technologies	Advanced gas turbine engine technologies	Positioning, navigation, and timing (PNT) technologies	Satellite networks (BeiDou)
Agricultural technologies			
	Renewable energy generation and storage	Clean energy generation and storage	Hydrogen energy, energy storage
AI	AI	AI	New generation AI, “Metaverse”
Autonomous systems	Autonomous systems and robotics	Highly automated, autonomous, and uncrewed systems and robotics	New energy vehicles, Internet of Vehicles
Biotechnologies	Biotechnologies	Biotechnologies	Biotechnologies
Chemical, biological, radiological, and nuclear (CBRN) mitigation technologies			
Communication and networking technologies	Communication and networking technologies	Integrated communication and networking technologies	Future networks, 5G, 6G
Data science and storage		Data Privacy, Data Security, and Cybersecurity Technologies	Big Data
Distributed ledger technologies	Financial technologies		Blockchain, “bioeconomy”
Energy Technologies	Directed energy, advanced nuclear energy technologies	Directed energy	New energy
Human-machine interfaces	Human-machine interfaces	Human-machine interfaces	“Brain-computer fusion”
Medical and public health technologies			Genetic technology, synthetic biology
QSI	QSI technologies	QSI technologies	QSI
Semiconductors and microelectronics	Semiconductors and microelectronics	Semiconductors and microelectronics	Integrated circuits
Space technologies	Space technologies and systems	Space technologies and systems	Deep-sea and aerospace development

* China’s CET list is not an official record but rather an aggregation of information from the State Council’s “Made in China 2025” plan, the NDRC’s National Guidelines, and the 14th FYP.

Notes

1. George F. Kennan, "Containment Then and Now," *Foreign Affairs* 65 (1987): 885–90.
2. Vojtech Mastny, *The Cold War and Soviet Insecurity: The Stalin Years* (Oxford University Press, 1996).
3. Leonid Brezhnev, "Brezhnev Doctrine," International Relations and Security Network, November 1968, <https://loveman.sdsu.edu/docs/1968BrezhnevDoctrine.pdf>.
4. "Fact Sheet: The Biden-Harris Administration's Abiding Commitment to Democratic Renewal at Home and Abroad," The White House, March 29, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-the-biden-harris-administrations-abiding-commitment-to-democratic-renewal-at-home-and-abroad/>.
5. Examples of such security pacts include the Quadrilateral Security Dialogue with Japan, India, and Australia, and the AUKUS Indo-Pacific partnership with Australia and the UK.
6. "China's National Defense in the New Era," State Council of the People's Republic of China, July 14, 2019, https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.
7. Trevor Hunnicutt and Nandita Bose, "Exclusive: Biden Aides in Talks with Vietnam for Arms Deal That Could Irk China," Reuters, September 23, 2023, <https://www.reuters.com/world/biden-aides-talks-with-vietnam-arms-deal-that-could-irk-china-2023-09-23/>.
8. G. John Ikenberry, "Power and Liberal Order: America's Postwar World Order in Transition," *International Relations of the Asia-Pacific* 5, no. 2 (2005): 133–52, <https://doi.org/10.1093/irap/lci112>.
9. "Xi Jinping's Speech via Video Link at Boao Forum for Asia (BFA) Annual Conference 2021," CGTN, April 20, 2021, <https://news.cgtn.com/news/2021-04-20/Full-text-Xi-Jinping-s-speech-at-BFA-Annual-Conference-2021-ZBRd9uTb0c/index.html>.
10. "US Trade with China 2022," Bureau of Industry and Security, accessed March 8, 2024, <https://www.bis.doc.gov/index.php/country-papers/3268-2022-statistical-analysis-of-u-s-trade-with-china/file>.
11. "China Imports by Country," Trading Economics, accessed June 6, 2024, <https://tradingeconomics.com/china/imports-by-country>.
12. "China Exports by Country," Trading Economics, accessed June 6, 2024, <https://tradingeconomics.com/china/exports-by-country>.
13. Eugene K. Keefe, *Soviet Union : A Country Study* (Federal Research Division, Library of Congress, 1991).
14. "National Strategy for Critical and Emerging Technologies," The White House, October 2020, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf>.
15. Fast Track Action Subcommittee on Critical and Emerging Technologies, *2022 Critical and Emerging Technologies List Update* (National Science and Technology Council, 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf>.
16. Fast Track Action Subcommittee on Critical and Emerging Technologies, *2024 Critical and Emerging Technologies List Update* (National Science and Technology Council, 2024), <https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf>.

17. “Made in China 2025’ Plan Issued,” State Council of the People’s Republic of China, May 2015, https://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm.
18. “New Chinese Ambitions for ‘Strategic Emerging Industries,’ Translated,” Center for Security and Emerging Technology, September 29, 2020, <https://cset.georgetown.edu/publication/new-chinese-ambitions-for-strategic-emerging-industries-translated/>.
19. “14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035, Translated,” Center for Security and Emerging Technology, May 2021, https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf.
20. This excludes China’s 14th FYP chapter on China’s civil-military fusion reform, which discusses dual development in ocean, aerospace, cyberspace, biology, new energy, AI, and quantum communication and computing.
21. “Xinhua Headlines-Xi Focus: Reshaping China’s Armed Forces,” Xinhua, accessed September 1, 2024, http://www.xinhuanet.com/english/2019-07/31/c_138273335.htm.
22. “The Chinese Communist Party’s Military-Civil Fusion Policy,” US Department of State, 2020, <https://2017-2021.state.gov/military-civil-fusion/index.html>.
23. “China’s Military Strategy,” Ministry of National Defense, May 2015, <http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html>.
24. In comparison, the DoD’s 2022 National Defense Strategy specifies nine technologies that could challenge strategic stability: counterspace weapons, hypersonics, advanced chemical and biological weapons, delivery systems, new applications of AI, quantum science, autonomy, biotechnologies, and space technologies.
25. NATO Science & Technology Organization, *Science & Technology Trends 2020–2040* (2020), https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.
26. “Summary of the 2018 National Defense Strategy,” US Department of Defense, 2018, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
27. Alexis G. Grynkewich, “Introducing Information as a Joint Function,” *Joint Force Quarterly* 89 (2018): 6–7.
28. “JP 3-04, Information in Joint Operations,” Joint Chiefs of Staff, September 2022.
29. “Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven),” Deputy Secretary of Defense, April 2017, https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf.
30. Katrina Manson, “AI Warfare Becomes Real for US Military with Project Maven,” Bloomberg, February 28, 2024, <https://www.bloomberg.com/features/2024-ai-warfare-project-maven/>.
31. China State Council, “Next Generation Artificial Intelligence Development Plan,” *China Science & Technology Newsletter* no. 17 (2017).
32. State Council of the People’s Republic of China, “China’s National Defense in the New Era.”
33. “Military and Security Developments Involving the People’s Republic of China,” US Department of Defense, October 2023, <https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-military-and-security-developments-involving-the-peoples-republic-of-china.pdf>.
34. “PLA Information Support Force Significant in Promoting High-Quality Development of Chinese Military and Winning Modern Warfare: Commentary,” *Global Times*, April 20, 2024, <https://www.globaltimes.cn/page/202404/1310942.shtml>.
35. John D. Blom, *Unmanned Aerial Systems: A Historical Perspective* (Combat Studies Institute Press, 2010).
36. Robyn Dixon, “Azerbaijan’s Drones Owned the Battlefield in Nagorno-Karabakh—and

- Showed Future of Warfare,” *Washington Post*, November 12, 2020, https://www.washingtonpost.com/world/europe/nagorno-karabakh-drones-azerbaijan-aremenia/2020/11/11/441b-cbd2-193d-11eb-8bda-814ca56e138b_story.html.
37. Stacie Pettyjohn, *Evolution Not Revolution: Drone Warfare in Russia’s 2022 Invasion of Ukraine* (Center for a New American Security, 2024).
 38. “China’s Calculus on Hypersonic Glide,” SIPRI, August 15, 2017, <https://www.sipri.org/commentary/topical-background/2017/chinas-calculus-hypersonic-glide>.
 39. Saylor M. Kelley, “Emerging Military Technologies: Background and Issues for Congress,” Congressional Research Service, February 2024, <https://sgp.fas.org/crs/natsec/R46458.pdf>.
 40. “Remarks by President Trump at Event Establishing the US Space Command,” US Space Command, August 29, 2019, <https://www.spacecom.mil/Newsroom/Speeches/Speech-Display/Article/2388821/remarks-by-president-trump-at-event-establishing-the-us-space-command/>.
 41. “About Space Force,” US Space Force, accessed June 5, 2024, <https://www.spaceforce.mil/About-Us/About-Space-Force/>.
 42. Saltzman Chance, “White Paper on Competitive Endurance: A Proposed Theory of Success for the US Space Force,” United States Space Force, January 2024, https://www.spaceforce.mil/Portals/2/Documents/White_Paper_Summary_of_Competitive_Endurance.pdf.
 43. “How Elon Musk’s Satellites Have Saved Ukraine and Changed Warfare,” *The Economist*, January 5, 2023, <https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare>.
 44. “Competing in Space, Second Edition,” National Space Intelligence Center and National Air and Space Center, December 2023, https://www.spoc.spaceforce.mil/Portals/4/Images/2_Space_Slicky_11x17_Web_View_reduced.pdf.
 45. National Space Intelligence Center and National Air and Space Center, “Competing in Space.”
 46. David Shepardson, “US Official Says Chinese Seizure of TSMC in Taiwan Would Be ‘Absolutely Devastating,’” *Yahoo Finance*, May 9, 2024, <https://finance.yahoo.com/news/us-official-says-chinese-seizure-151702299.html>.
 47. Amy Spiro, “Pompeo Says F-35 Sale to UAE Was ‘Critical’ to the Abraham Accords,” *Times of Israel*, June 10, 2021, <https://www.timesofisrael.com/pompeo-says-f-35-sale-to-uae-was-critical-to-the-abraham-accords/>.
 48. “2022 National Defense Strategy of the United States of America,” US Department of Defense, October 2022, <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-national-defense-strategy-npr-mdr.pdf>.
 49. “National Cybersecurity Strategy,” The White House, March 2023, <https://www.cybercom.mil/Portals/56/Documents/Mission%20and%20Vision/National-Cybersecurity-Strategy-2023.pdf>.
 50. James Pamment et al., “Hybrid Threats: 2007 Cyber Attacks on Estonia,” NATO StratCom COE, June 6, 2019, <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>.
 51. “Summary: 2023 DoD Cyber Strategy,” US Department of Defense, September 2023, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.
 52. “CIA Releases Report ‘US Threats and Sabotage to the Security and Development of Global Cyberspace,’” *China Daily*, April 28, 2024, <https://www.chinadaily.com.cn/a/202404/28/WS662e4067a31082fc043c47dc.html>.
 53. The White House, “National Cybersecurity Strategy.”

54. “The Privacy Project,” *New York Times*, April 10, 2019, sec. Opinion, <https://www.nytimes.com/interactive/2019/opinion/internet-privacy-project.html>.
55. Ellen Nakashima, “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say,” *Washington Post*, December 1, 2021, <https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>.
56. *New York Times*, “The Privacy Project.”
57. “Annual Threat Assessment of the US Intelligence Community,” Office of the Director of National Intelligence, February 5, 2024, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>.
58. On April 19, 2024, the Strategic Support Force was dissolved and split into three independent arms: the PLA Aerospace Force, the PLA Cyberspace Force, and the PLA Information Support Force.
59. US Department of Defense, “Military and Security Developments.”
60. Ken Dilanian, “FBI Director Says Agency Is Sharing Intelligence to Prevent Violence on College Campuses over Israel-Hamas War,” NBC News, April 23, 2024, <https://www.nbc-news.com/politics/national-security/fbi-director-says-agency-sharing-intelligence-prevent-violence-college-rcna149018>.
61. Katerina E. Matsa, “More Americans Are Getting News on TikTok, Bucking the Trend Seen on Most Other Social Media Sites,” Pew Research Center, November 15, 2023, <https://www.pewresearch.org/short-reads/2023/11/15/more-americans-are-getting-news-on-tiktok-bucking-the-trend-seen-on-most-other-social-media-sites/>.
62. Noah Berman, Lindsay Maizland, and Andrew Chatzky, “Is China’s Huawei a Threat to US National Security?,” Council on Foreign Relations, February 8, 2023, <https://www.cfr.org/background/chnas-huawei-threat-us-national-security>.
63. “5G Security,” *Schneier on Security* (blog) January 14, 2020, https://www.schneier.com/blog/archives/2020/01/china_isnt_the_.html.
64. “FCC Designates Huawei and ZTE as National Security Threats,” Federal Communications Commission, June 30, 2020, <https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats>.
65. “Fact Sheet: President Biden Issues Executive Order to Protect Americans’ Sensitive Personal Data,” The White House, February 28, 2024, <https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/>.
66. Brian Fung, “Biden Just Signed a Potential TikTok Ban into Law. Here’s What Happens Next,” CNN, April 24, 2024, <https://www.cnn.com/2024/04/23/tech/congress-tiktok-ban-what-next/index.html>.
67. Robin Wauters, “China Blocks Access to Twitter, Facebook after Riots,” *Washington Post*, July 7, 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/07/07/AR2009070701162.html>.
68. *China Daily*, “CCIA Releases Report.”
69. US Department of Defense, “Military and Security Developments.”
70. “National Security Memorandum on Promoting United States Leadership in Quantum Computing while Mitigating Risks to Vulnerable Cryptographic Systems,” The White House, May 4, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing>

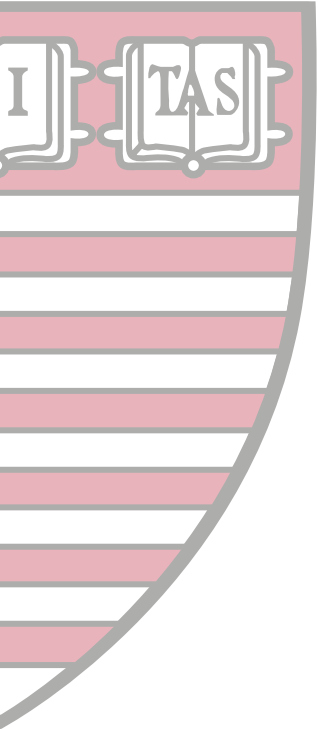
- [-while-mitigating-risks-to-vulnerable-cryptographic-systems/](#).
71. David Lague, “US and China Race to Shield Secrets from Quantum Computers,” Reuters, December 14, 2023, <https://www.reuters.com/investigates/special-report/us-china-tech-quantum/>.
 72. Joseph S. Nye Jr., “Mikhail Gorbachev and the End of the Cold War,” Project Syndicate, March 28, 2006, <https://www.project-syndicate.org/commentary/mikhail-gorbachev-and-the-end-of-the-cold-war>.
 73. “The Fourth Industrial Revolution: What It Means and How to Respond,” World Economic Forum, January 14, 2016, <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>.
 74. National Security Commission on Artificial Intelligence, *NSCAI Final Report* (2021), <https://reports.nscai.gov/final-report/>.
 75. President’s Council of Advisors on Science and Technology, *Report to the President: Supercharging Research: Harnessing Artificial Intelligence to Meet Global Challenges* (2024), https://www.whitehouse.gov/wp-content/uploads/2024/04/AI-Report_Upload_29APRIL2024_SEND-2.pdf.
 76. Kristalina Georgieva, “AI Will Transform the Global Economy. Let’s Make Sure It Benefits Humanity,” *IMF Blog*, January 14, 2024, <https://www.imf.org/en/Blogs/Articles/2024/01/14/ai-will-transform-the-global-economy-lets-make-sure-it-benefits-humanity>.
 77. Michael Chui et al., *The Economic Potential of Generative AI* (McKinsey & Company, 2023), <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier>.
 78. Ben Buchanan, “The AI Triad and What It Means for National Security Strategy,” Center for Security and Emerging Technology, August 2020, <https://doi.org/10.51593/20200021>.
 79. Jared Cohen and George Lee, “The Generative World Order: AI, Geopolitics, and Power,” Goldman Sachs, December 14, 2023, <https://www.goldmansachs.com/intelligence/pages/the-generative-world-order-ai-geopolitics-and-power.html>.
 80. “Interim Measures for the Management of Generative Artificial Intelligence Services,” *China Law Translate* (blog), July 13, 2023, <https://www.chinalawtranslate.com/generative-ai-interim/>.
 81. Cohen and Lee, “The Generative World Order.”
 82. Meaghan Tobin, “China Announces Rules to Keep AI Bound by ‘Core Socialist Values,’” *Washington Post*, July 14, 2023, <https://www.washingtonpost.com/world/2023/07/14/china-ai-regulations-chatgpt-socialist/>.
 83. Lotus Ruan, “Big Data in China and the Battle for Privacy,” Australian Strategic Policy Institute, June 22, 2018, <http://www.aspi.org.au/report/big-data-china-and-battle-privacy>.
 84. Isabelle Qian et al., “Four Takeaways from a Times Investigation Into China’s Expanding Surveillance State,” *New York Times*, June 21, 2022, sec. World, <https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html>.
 85. Chen Yurong and Liu Wei, “Four Takeaways from China’s Newly Planned National Data Bureau,” CGTN, March 9, 2023, <https://news.cgtn.com/news/2023-03-08/Four-takeaways-from-China-s-newly-planned-national-data-bureau-1i0MqUHCMSI/index.html>.
 86. Ondrej Burkacku et al., “AI in Semiconductor Manufacturing: The Next S Curve?,” McKinsey & Company, March 29, 2024, <https://www.mckinsey.com/industries/semiconductors/our-insights/generative-ai-the-next-s-curve-for-the-semiconductor-industry>.

87. “Fact Sheet: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China,” The White House, August 9, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/>.
88. Akhil Thadani and Gregory C. Allen, “Mapping the Semiconductor Supply Chain: The Critical Role of the Indo-Pacific Region,” Center for Strategic and International Studies, May 2023, <https://www.csis.org/analysis/mapping-semiconductor-supply-chain-critical-role-indo-pacific-region>.
89. “NVIDIA Blackwell Platform Arrives to Power a New Era of Computing,” Nvidia, March 18, 2024, <https://nvidianews.nvidia.com/news/nvidia-blackwell-platform-arrives-to-power-a-new-era-of-computing>.
90. Thadani and Allen, “Mapping the Semiconductor Supply Chain.”
91. “Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration’s National Security Strategy,” The White House, October 13, 2022, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-national-security-strategy/>.
92. Ana Swanson, “Netherlands and Japan Said to Join US in Curbing Chip Technology Sent to China,” *New York Times*, January 28, 2023, sec. Business, <https://www.nytimes.com/2023/01/28/business/economy/netherlands-japan-china-chips.html>.
93. “Japan, US, South Korea, Taiwan Launch ‘Chip 4’ Talks for Supply Chain,” Kyodo News, February 27, 2023, <https://english.kyodonews.net/news/2023/02/fb77092264b1-japan-us-s-korea-taiwan-launch-chip-4-talks-for-supply-chain.html>.
94. “FM Spokesperson: China Firmly Opposes US Restrictions on Investments in China,” State Council Information Office, August 10, 2023, http://english.scio.gov.cn/press-room/2023-08/10/content_100922410.htm.
95. Milton Ezrati, “How Much Control Does China Have Over Rare Earth Elements?,” *Forbes*, December 11, 2023, <https://www.forbes.com/sites/miltonezrati/2023/12/11/how-much-control-does-china-have-over-rare-earth-elements/>.
96. Reed Blackmore, “What to Make of China’s Latest Restrictions on Critical Mineral Exports,” *New Atlanticist* (blog), October 26, 2023, <https://www.atlanticcouncil.org/blogs/new-atlanticist/what-to-make-of-chinas-latest-restrictions-on-critical-mineral-exports/>.
97. Song Wei, “Huawei’s Mate 60 Pro a Remarkable Breakthrough,” *China Daily*, September 26, 2023, <https://www.chinadaily.com.cn/a/202309/26/WS6512175da310d2dce4bb7c01.html>.
98. “Compare Huawei Mate 60 vs Apple iPhone 15: Which Is Better?,” NanoReview, accessed June 17, 2024, <https://nanoreview.net/en/phone-compare/huawei-mate-60-vs-apple-iphone-15>.
99. “Apple’s 3nm iPhone Chip Advantage (and Why It Doesn’t Really Matter),” Macworld, accessed June 9, 2024, <https://www.macworld.com/article/1446844/3nm-processor-advantage-qualcomm-mediatek-tsmc.html>.
100. “High-Performance Computing,” Nvidia, accessed June 11, <https://www.nvidia.com/en-eu/glossary/high-performance-computing/>.
101. Eric Schmidt, “Why Technology Will Define the Future of Geopolitics,” *Foreign Affairs*, February 28, 2023, <https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics>.
102. Alex Heath, “Mark Zuckerberg’s New Goal Is Creating Artificial General Intelligence,” *The*

- Verge, January 18, 2024, <https://www.theverge.com/2024/1/18/24042354/mark-zuckerberg-meta-agi-reorg-interview>.
103. Charlie Campbell, “Why China, the US, and Big Tech Are Racing to Harness Quantum Computing and AI,” *Time*, May 13, 2024, <https://time.com/6977355/generative-ai-quantum-computing-us-china-technology/>.
 104. Kif Leswing, “Intel Says Moore’s Law Is Still Alive and Well. Nvidia Says It’s Ended,” CNBC, September 27, 2022, <https://www.cnbc.com/2022/09/27/intel-says-moores-law-is-still-alive-nvidia-says-its-ended.html>.
 105. “What Is Quantum Computing?,” McKinsey, April 5, 2024, <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing>.
 106. Matt Langione et al., “Quantum Computing Is Becoming Business Ready,” BCG Global, April 27, 2023, <https://www.bcg.com/publications/2023/enterprise-grade-quantum-computing-almost-ready>.
 107. Michael Bogobowicz et al., “Quantum Technology Monitor,” McKinsey & Company, April 2024, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage#.
 108. Langione et al., “Quantum Computing Is Becoming Business Ready.”
 109. Sam Howell, “The China-US Quantum Race,” *The Diplomat*, January 13, 2023, <https://thediplomat.com/2023/01/the-china-us-quantum-race/>.
 110. Center for Security and Emerging Technology, “14th Five-Year Plan.”
 111. Michael Bogobowicz et al., “Quantum Technology Monitor.”
 112. “Interim Report,” National Security Commission on Emerging Biotechnology, January 10, 2024, <https://www.biotech.senate.gov/press-releases/interim-report/>.
 113. “Biomanufacturing to Advance the Bioeconomy,” President’s Council of Advisors on Science and Technology, December 2022, https://www.whitehouse.gov/wp-content/uploads/2022/12/PCAST_Biomanufacturing-Report_Dec2022.pdf.
 114. Michael Chui et al., “The Bio Revolution: Innovations Transforming Economies, Societies, and Our Lives,” McKinsey, May 13, 2020, <https://www.mckinsey.com/industries/life-sciences/our-insights/the-bio-revolution-innovations-transforming-economies-societies-and-our-lives>.
 115. François Candelon et al., “What’s Your Synthetic Biology Strategy?,” BCG Global, February 15, 2023, <https://www.bcg.com/publications/2023/what-is-your-synthetic-bio-strategy>.
 116. Office of the Director of National Intelligence, “Annual Threat Assessment of the US Intelligence Community.”
 117. Eric Martin, “US Wants to ‘De-Risk,’ Not Decouple, from China, Biden Aide Says,” *Bloomberg*, April 27, 2023, <https://www.bloomberg.com/news/articles/2023-04-27/us-wants-to-de-risk-not-decouple-from-china-biden-aide-says>.
 118. “Fact Sheet: President Biden to Launch a National Biotechnology and Biomanufacturing Initiative,” The White House, September 12, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/12/fact-sheet-president-biden-to-launch-a-national-biotechnology-and-biomanufacturing-initiative/>.
 119. The White House, *Bold Goals for US Biotechnology and Biomanufacturing: Harnessing Research and Development to Further Societal Goals* (2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/Bold-Goals-for-US-Biotechnology-and-Biomanufacturing-Harnessing-Research-and-Development-To-Further-Societal-Goals-FINAL.pdf>.
 120. The White House, *Bold Goals for US Biotechnology and Biomanufacturing*.

121. “China’s Biotechnology Development: The Role of US and Other Foreign Engagement,” Gryphon Scientific and Rhodium Group, February 14, 2019, <https://www.uscc.gov/sites/default/files/Research/US-China%20Biotech%20Report.pdf>.
122. Center for Security and Emerging Technology, “14th Five-Year Plan.”
123. Gryphon Scientific and Rhodium Group, “China’s Biotechnology Development.”
124. “China Genomics Factsheet,” National Counterintelligence and Security Center, February 2021, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf.
125. Joby Warrick and Cate Brown, “China’s Quest for Human Genetic Data Spurs Fears of a DNA Arms Race,” *Washington Post*, October 19, 2023, <https://www.washingtonpost.com/world/interactive/2023/china-dna-sequencing-bgi-covid/>.
126. National Counterintelligence and Security Center, “China Genomics Factsheet.”
127. Warrick and Brown, “China’s Quest for Human Genetic Data Spurs Fears of a DNA Arms Race.”
128. Kirsty Needham and Clare Baldwin, “China’s Gene Giant Harvests Data from Millions of Pregnant Women,” Reuters, July 7, 2021, <https://www.reuters.com/investigates/special-report/health-china-bgi-dna/>.
129. National Security Commission on Emerging Biotechnology, “Interim Report.”
130. Ken Dilanian, “Congress Wants to Ban China’s Largest Genomics Firm from the US Here’s Why,” NBC News, January 25, 2024, <https://www.nbcnews.com/politics/national-security/congress-wants-ban-china-genomics-firm-bgi-from-us-rcna135698>.
131. Didi Tang, “US Rivalry with China Expands to Biotech. Lawmakers See a Failure to Compete and Want to Act,” AP News, February 18, 2024, <https://apnews.com/article/us-biotechnology-biotech-china-congress-communist-party-c892d9d18d8f38dad7e-955fa8038e7d6>.
132. Pallab Ghosh, “China’s New Human Gene-Editing Rules Worry Experts,” BBC, March 6, 2023, <https://www.bbc.com/news/science-environment-64857311>.
133. Françoise Baylis et al., “Human Germline and Heritable Genome Editing: The Global Policy Landscape,” *CRISPR Journal* 3, no. 5 (2020): 365–77, <https://doi.org/10.1089/crispr.2020.0082>.
134. Joshua Park, “Breaking the Internet: China-US Competition Over Technology Standards,” *The Diplomat*, February 9, 2022, <https://thediplomat.com/2022/02/breaking-the-internet-china-us-competition-over-technology-standards/>.
135. “National Standards Strategy for Critical and Emerging Technology,” The White House, May 2023, <https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf>.
136. “Form 10-K,” Qualcomm Incorporated, FY 2023, <https://investor.qualcomm.com/financial-information/sec-filings/content/0000804328-23-000055/0000804328-23-000055.pdf>.
137. Tim Rühlig, “China, Europe and the New Power Competition over Technical Standards,” UI Brief No. 1, Swedish Institute of International Affairs, 2021.
138. Jeff Okun-Kozlowicki, “Standards and Regulations: Measuring the Link to Goods Trade,” Office of Standards and Investment Policy, June 2016, https://legacy.trade.gov/td/osip/documents/osip_standards_trade_full_paper.pdf.
139. Rühlig, “China, Europe and the New Power Competition.”
140. Rühlig, “China, Europe and the New Power Competition.”
141. Emily de La Bruyère and Nathan Picarsic, *China Standards 2035* (Horizon Advisory, 2020), <https://www.horizonadvisory.org/china-standards-2035-first-report>.

142. “The Chinese Communist Party Central Committee and the State Council Publish the ‘National Standardization Development Outline,’” Center for Security and Emerging Technology, November 19, 2021, <https://cset.georgetown.edu/publication/the-chinese-communist-party-central-committee-and-the-state-council-publish-the-national-standardization-development-outline/>.
143. Park, “Breaking the Internet.”
144. Valentina Pop, Sha Hua, and Daniel Michaels, “From Lightbulbs to 5G: China Battles West for Control of Vital Technology Standards,” *Wall Street Journal*, February 7, 2021, sec. World, <https://www.wsj.com/articles/from-lightbulbs-to-5g-china-battles-west-for-control-of-vital-technology-standards-11612722698>.
145. Ashwani Sharma et al., “Artificial Intelligence-Based Data-Driven Strategy to Accelerate Research, Development, and Clinical Trials of COVID Vaccine,” *BioMed Research International* (2022): 1–16, <https://doi.org/10.1155/2022/7205241>.
146. Peter Martin and Jenny Leonard, “The US Keeps Offering China Its COVID Vaccines. China Keeps Saying No,” *Time*, accessed January 6, 2023, <https://time.com/6245054/us-china-covid-vaccines/>.
147. Michael Martina and David Brunnstrom, “China’s Xi Unwilling to Accept Western Vaccines, US Official Says,” Reuters, December 5, 2022, <https://www.reuters.com/world/china/chinas-xi-unwilling-accept-vaccines-despite-threat-protests-us-intel-2022-12-04/>.
148. “WHO Validates Sinovac COVID-19 Vaccine for Emergency Use and Issues Interim Policy Recommendations,” World Health Organization, June 1, 2021, <https://www.who.int/news/item/01-06-2021-who-validates-sinovac-covid-19-vaccine-for-emergency-use-and-issues-interim-policy-recommendations>.
149. US Mission China, “COVID-19 Information,” US Embassy and Consulates in China, January 27, 2023, <https://china.usembassy-china.org.cn/covid-19-information/>.
150. Matthew Cranston, “The \$183b COVID Boom Is Turning to Bust for Pfizer and Moderna,” *Financial Review*, August 21, 2023, <https://www.afr.com/companies/healthcare-and-fitness/pfizer-moderna-shares-under-pressure-as-covid-19-vaccine-sales-fade-20230821-p5dy1z>.
151. “WTO-IMF Vaccine Trade Tracker,” World Trade Organization, accessed June 11, 2024, https://www.wto.org/english/tratop_e/covid19_e/vaccine_trade_tracker_e.htm.
152. Josep Borrell, “Vaccinating the World: Between Promises and Realities,” EEAS, June 19, 2022, https://www.eeas.europa.eu/eeas/vaccinating-world-between-promises-and-realities_en.
153. Cheng Ting-Fang and Shunsuke Tabeta, “Tesla Cars Face More Entry Bans in China as ‘Security Concerns’ Accelerate,” *Nikkei Asia*, January 24, 2024, <https://asia.nikkei.com/Spotlight/Supply-Chain/Tesla-cars-face-more-entry-bans-in-China-as-security-concerns-accelerate>.
154. “Fact Sheet: Biden-Harris Administration Takes Action to Address Risks of Autos from China and Other Countries of Concern,” The White House, February 29, 2024, <https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/29/fact-sheet-biden-harris-administration-takes-action-to-address-risks-of-autos-from-china-and-other-countries-of-concern/>.
155. David Shepardson, “US Could Ban Chinese Connected Vehicles or Impose Restrictions,” Reuters, May 8, 2024, sec. United States, <https://www.reuters.com/world/us/us-could-ban-chinese-connected-vehicles-or-impose-restrictions-us-commerce-2024-05-08/>.



A PUBLICATION OF THE
Rajawali Foundation Institute for Asia
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

rajawali.hks.harvard.edu



HARVARD Kennedy School

RAJAWALI FOUNDATION INSTITUTE FOR ASIA