



U.S.-China Economic and Security Review Commission

2026 Report to Congress

Executive Summary and Recommendations





2026
REPORT TO CONGRESS

U.S.-China Economic and Security Review Commission

Executive Summary and Recommendations

One Hundred Nineteenth Congress
Second Session
November 2026

Printed for the use of the
U.S.-China Economic and Security Review Commission

Digital copies of the full 2026 Annual Report to Congress and this Executive Summary are available online at: **www.USCC.gov**

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

COMMISSIONERS

Hon. Randall Schriver	Chair
Mike Kuiken	Vice Chair

Hal Brands	**Reva Price** (Chair Emeritus)
Taylor Budowich	**Livia Shmavonian**
Joshua Hodges	**Chris Slevin**
Leland R. Miller	**Hon. Jonathan N. Stivers**

2026 COMMISSION STAFF

Michael Castellano	Executive Director
Christopher P. Fioravante	Deputy Executive Director
Graham E. Ayres	Policy Analyst, Economics and Trade
Rachael Burton	Research Manager & Senior Policy Analyst, Security and Foreign Affairs
Jameson Cunningham	Director, Congressional Affairs and Communications
Joseph Federici	Senior Policy Analyst, Security and Foreign Affairs
Benton Gordon	Policy Analyst, Economics and Trade
Kathleen Hawk	Director, Security and Foreign Affairs
Zoe Merewether	Acting Director, Economics and Trade
Eric Omorogieva	Policy Analyst, Economics and Trade & Technology and Innovation
Morgan Peirce	Policy Analyst, Security and Foreign Affairs & Technology and Innovation
Matthew Sperzel	Policy Analyst, Security and Foreign Affairs
Meghan Sullivan	Congressional Affairs and Communications Assistant
Evan J. Ulman	Administrative and Outreach Coordinator
Emily S. Weinstein	Director, Technology and Innovation

The Commission, a legislative branch entity, was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act of 2001, Pub. L. No. 106-398 (codified at 22 U.S.C. § 7002), as amended by: The Treasury and General Government Appropriations Act, 2002, Pub. L. No. 107-67 (Nov. 12, 2001); The Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7 (Feb. 20, 2003); The Science, State, Justice, Commerce, and Related Agencies Appropriations Act, 2006, Pub. L. No. 109-108 (Nov. 22, 2005); The Consolidated Appropriations Act, 2008, Pub. L. No. 110-161 (Dec. 26, 2007); The Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291 (Dec. 19, 2014); and Pub. L. No. 117-286 (Dec. 27, 2022). The Commission's full charter and statutory mandate are available online at: www.USCC.gov/charter.

Cover photo credit: Manta Ray uncrewed underwater vehicle, Northrop Grumman (the appearance of visual information from Northrop Grumman and/or the Department of Defense does not imply or constitute endorsement); binary code, Getty Images; Port of Chancay in Peru, Getty Images; bauxite and iron ore in China's Shandong province, Getty Images.

TABLE OF **CONTENTS**

6 **TRANSMITTAL LETTER**

8 **INTRODUCTION**

11 **THE COMMISSION'S KEY RECOMMENDATIONS**

16 **EXECUTIVE SUMMARY**

16 **Part I: The Year in Review**

16 Chapter 1: U.S.-China Economic and Trade Relations

18 Chapter 2: U.S.-China Security and Foreign Affairs

21 **Part II: China's Efforts to Expand Its Global Power and Influence**

21 Chapter 3: China's Other Front: India and the Future of U.S. Strategy in the Indo-Pacific

24 Chapter 4: China's Predatory Diplomacy in Latin America: Broken Promises, Harmful Practices

27 Chapter 5: Active Intercept: China's Efforts to Narrow U.S. Undersea Advantage

30 Chapter 6: The Price of Everything: China's Bid to Reshape Global Commodities Markets

33 **Part III: China's Technology Ambitions**

33 Chapter 7: Collect, Steal, Buy, Fuse, Monetize: How China Is Turning Data into Assets and Ammunition

36 Chapter 8: Silicon to Sovereignty: China's Bid to Control the AI Stack from Wafer to Weights, Part One

38 **Part IV: Taiwan and Hong Kong**

38 Chapter 9: Taiwan: A Crucial Window for a Critical Partner

41 Chapter 10: Hong Kong: Enabler of China's Global Finance and Technology Ambitions

44 **COMPREHENSIVE LIST OF RECOMMENDATIONS**

U.S.-China Economic and Security Review Commission

November 18, 2026

The Honorable Charles E. Grassley
President Pro Tempore of the U.S. Senate, Washington, DC 20510

The Honorable Mike Johnson
Speaker of the U.S. House of Representatives, Washington, DC 20510

Dear Senator Grassley and Speaker Johnson:

On behalf of the U.S.-China Economic and Security Review Commission, we are pleased to transmit the Commission's 2026 Annual Report to Congress. This Report responds to our mandate "to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China." The Commission reached a broad and bipartisan consensus on the contents of this Report, with all 10 members (two appointments remain vacant) voting unanimously to approve and submit it to Congress.

In accordance with our mandate, this Report, which is current as of October 8, 2026, includes the results and recommendations of our hearings, research, and review of the areas identified by Congress in our mandate, as defined in Public Law No. 106–398 (October 30, 2000) and amended by Public Laws No. 107–67 (November 12, 2001), No. 108–7 (February 20, 2003), 109–108 (November 22, 2005), No. 110–161 (December 26, 2007), No. 113–291 (December 19, 2014), and No. 117-286 (December 27, 2022). The Commission's charter, which includes the 11 directed research areas of our mandate, is included as Appendix I of the Report.

The Commission conducted five public hearings, taking testimony from 35 expert witnesses from government, the private sector, academia, think tanks, research institutions, and other backgrounds. For each of these hearings, the Commission produced a transcript (posted on our website at *www.USCC.gov*). This year's hearings included:

- India, China, and the Balance of Power in the Indo-Pacific
- Part of Your World: U.S.-China Competition Under the Sea
- China's Expanding Interests in Latin America: Development, Leverage, Coercion, and Crime
- Pricing the Future: China's Ambitions for Commodity Derivatives Markets
- Taking a Bigger Byte: China's Expanding Strategy for Data Dominance

The Commission received a number of briefings, both unclassified and classified, by executive branch agencies, the U.S. military, the intelligence community, foreign government officials, and U.S. and foreign nongovernmental experts on a range of topics within the Commission's mandate. The Commission includes key insights gained through these briefings either in its unclassified Annual Report or, as appropriate, in a classified annex to that Report.

The Commission conducted official fact-finding travel this year to Beijing, Hangzhou, and Shanghai, China, its first official travel to the country since 2019. The delegation held frank discussions with its interlocutors on a range of subjects, including artificial intelligence, advanced technology, biotechnology, local economic and business conditions, economic security, regional security, and global issues. The Commission also traveled to India, Panama, and Mexico to hear and discuss perspectives on China's economic, foreign policy, and security activities in each country and its region, U.S.-China relations, and efforts to reduce reliance on China in critical supply chains and infrastructure. Across these visits, Commission delegations met with U.S. diplomats, foreign government officials, think tanks, business representatives, academics, and other experts. Throughout the year, the Commission relied substantially on the work of our excellent professional staff and outside contracted research (see Appendix IV) in accordance with our mandate (see Appendix I).

The Report includes 30 recommendations for congressional consideration. The Commissioners agreed that ten of these recommendations, which appear on page 11, are the most important for congressional action. The complete list of recommendations appears on page 44 at the conclusion of the Executive Summary.

We offer this Report to Congress in the hope that it will be useful in helping guide policies to better address the economic and national security implications of the U.S.-China relationship, while advancing American interests and values. Thank you for the opportunity to serve. We look forward to continuing to work with Members of Congress in the upcoming year to address issues of concern in the U.S.-China relationship.

Sincerely,



Randall Schriver
Chair



Mike Kuiken
Vice Chair

INTRODUCTION

Twenty-five years ago, China stood at the threshold of joining the WTO and Washington debated whether further opening the U.S. market and commerce to China would liberalize Beijing. Congress made a decision to create the U.S.-China Economic and Security Review Commission, charging the Commission with the responsibility to monitor the economic and national security implications of opening trade and economic ties between the United States and the People's Republic of China. Each report—with its corresponding set of legislative recommendations—issued since has documented abuses by China and the failed delivery of its promises and commitments.

In 2026, the United States and China have entered into a new phase, pursuing what both governments have termed a "constructive relationship of strategic stability based on respect, fairness, and reciprocity," built on an unusually active schedule of leader-level engagement between President Donald J. Trump and General Secretary of the Chinese Communist Party (CCP) Xi Jinping. At their May summit in Beijing, the two leaders agreed to establish a Board of Trade to identify goods the two countries can trade without crossing national security red lines and to oversee reciprocal tariff reductions as well as a Board of Investment to address specific investment issues between the two countries. At their September summit in Washington, the two sides agreed to launch a U.S.-China dialogue on artificial intelligence (AI) and to establish a bilateral communication channel for AI-related incidents. Yet China's conduct over the last 25 years shows that Beijing's version of "stability" does not mean restraint. Even as these channels have opened and expanded, Chinese leaders have continued to use every instrument of state power—military, economic, technological, legal, and diplomatic—to gain advantage over the United States and other countries while managing the risk of a confrontation that could interrupt their progress.

Beijing has offered this kind of framing before as a tool for managing the United States, often successfully. There have been several iterations, including in the 1990s, when Chinese officials proposed building a "constructive strategic partnership." During the George W. Bush Administration, the formulation was a "candid, constructive, and cooperative" relationship; during the Obama Administration, a "new type of great power relations." Whatever the packaging, a bill is attached: mutual respect for China's so-called core interests, which in Beijing's usage means yielding to its demands on Taiwan, Tibet, Xinjiang, and the South China Sea. "Constructive strategic stability" is the same product in newer wrapping, and it carries the same bill. Beijing is not seeking to stabilize competition so much as proposing the terms by which the United States would compete less aggressively—and it has chosen a phrase that makes the concession sound like statesmanship.

China accelerated its bid to reshape the international order in 2026, intensifying a coercive but controlled strategy that used its growing military, technological, economic, and diplomatic power to strengthen its position relative to the United States. Even as Beijing sought to manage its diplomatic relationship with Washington, it continued to conduct cyber operations targeting U.S. critical infrastructure, ran AI-enhanced influence campaigns aimed at the American public, attempted to co-opt U.S. officials, and carried out transnational repression on U.S. soil.

Over the last year, China remained a critical enabler of Russia's war effort and Iran's military capacity, facilitating more than 90 percent of Russia's imports of sanctioned dual-use technology and supplying Iran with drone components and materials used to make missile fuel while carefully avoiding direct involvement in either conflict. Beijing has used the growing dependence of both partners to expand its own strategic leverage.

Across Latin America, commercial relationships that appear mutually beneficial convert into political leverage the moment a government asserts its own sovereignty: weeks after Panama's Supreme Court voided a Hong Kong company's port concessions, COSCO walked out of the port of Balboa, and Chinese authorities detained nearly 500 Panama-flagged vessels, driving 230 ships off the world's second-largest registry within two months. Similarly, the Commission learned that in addition to legitimate Chinese businesses in Latin American markets, there are often illicit Chinese-linked networks that facilitate local and transnational crime. Similar to the way China has responded to its role in the U.S. fentanyl crisis, it only selectively cooperates against these destabilizing activities.

These are not the behaviors of a co-manager. They are the behaviors of a power that treats every dependence as a weapon in waiting.

Building on our recent reports, the Commission's work this year gives renewed emphasis to the growing dependencies Beijing is building across critical sectors. The rare earth controls China exercised in 2025 were a demonstration of a model, not its limit. Beijing is working to replicate that chokepoint position wherever the world depends on it for an input—active pharmaceutical ingredients and their starting materials, mature-node chips, battery materials and technology, and precursor chemicals necessary in the production of many modern goods. In several of these sectors the position is nearly consolidated, which means the window for preventing the next round of leverage is closing rapidly. Over the last few years, the Commission has made various recommendations to reduce critical dependencies on Chinese supply chains, including ideas focused on the demand side of resilience and working in coordination with allies and partners to develop joint responses, rather than walls alone, to make sure secure supply is commercially viable.

Beijing is also writing rules for domains where none yet bind. Last year the Commission documented this approach in space; this year it found the same playbook beneath the sea, where China is trying to shape the International Seabed Authority's regulatory environment in pursuit of favorable commercial mining rules. Meanwhile, it is leveraging seabed exploration, scientific research, and emerging technologies, and mapping the seafloor along the Hawaii-to-Guam corridor and the approaches to the first island chain, in an attempt to narrow the U.S. undersea warfare advantage. In commodities, China is using consolidated state buying power to support alternative centers for exchanges, having already established the key commodity market for some products, like lithium, while compelling major iron ore producers off the established benchmark and toward its preferred pricing tools. In data, it is seeking to set the norms from the start: this year it launched a World Data Organization claiming members across 42 countries, reportedly enlisting the Chinese subsidiaries of American firms in the project. In the meantime, Washington still treats data in separate regulatory stovepipes. In each domain, the United States must contest the rules before they harden, because rules, once written, are a form of leverage for the authors that is difficult to unwind.

Nowhere are the stakes higher than Taiwan, where Beijing's aim is to win without fighting—applying gray-zone pressure, economic leverage, cyber operations, and political influence until the status quo has degraded far enough that its preferred outcome looks inevitable. This campaign has been underway for years, and the goalposts have already moved in China's favor. Taiwan is critical to American power in the Western Pacific, and its security is closely tied to allied confidence in U.S. commitments. Taiwan also produces the overwhelming majority of the leading-edge semiconductors powering the American artificial intelligence buildout, and it is equally vital for the foundational chips that run cars, appliances, medical devices, and weapons systems. The United States has spent decades building the capability to deter and defeat an invasion, and that work remains essential. We are less prepared for the alternatives China is openly exploring—blockade, quarantine, and coercion campaigns that put American geopolitical power and the world's semiconductor supply at risk without a single landing craft leaving port. This Report's analysis and recommendations address that gap directly.

The United States must compete for the countries Beijing insists do not matter. India is clear that it will not sit in any other country's camp, which is precisely why it matters so much in this competition—and why Beijing works so hard to keep India's industrial rise dependent on Chinese machinery,

components, and expertise. That vulnerability is not India's alone: when Beijing demanded that Indian firms respect its export controls against the United States, it turned India's dependence into a weapon aimed at American supply chains.

Over a quarter century, the Commission's reports documented China's failures to comply with its WTO commitments when the consensus view still hoped for convergence; the Commission warned of rare earth leverage, forced technology transfer, and military-civil fusion years before those terms entered common use, and it supplied evidentiary support for measures Congress ultimately enacted, from the modernization of foreign investment screening to audit-access requirements for listings of Chinese companies to import restrictions on goods made with forced labor. The Commission continues to update its research to measure Beijing's words against its actions and tell Congress plainly where the gaps lie. The competition is real. The task now is to win it.

That task has a calendar, and the coming year is crowded. In 2027, the People's Liberation Army marks its centennial—the milestone against which Xi Jinping has ordered the capabilities for a Taiwan contingency to be ready. The CCP convenes its 21st Party Congress, where Xi is expected to claim a fourth term. Hong Kong reaches the 30th anniversary of its handover, still two decades shy of China's 50-year autonomy commitment, which Beijing dismantled in its first 25. And the trade arrangements that paused escalation in 2025 are set to expire soon after this Report goes to print, potentially returning both capitals to a landscape of live leverage. None of these dates makes conflict inevitable. Each raises the premium on decisions taken now: deterrence, resilience, and allied cohesion are built in the quiet months, not summoned in the loud ones.

For more than a decade, Beijing has worked to position itself as a technological rival and alternative to the United States, and 2026 once again revealed how much of that position is built on American ingenuity and capital. That is the campaign Beijing hopes to materialize—to have the United States accept it as its only peer—because that concession would ratify the levers of control it is building and isolate America from the allies whose weight together has created the durable power and peace of the 21st century, clearing Beijing's path to the center of future progress.

The Commission submits this Report as the 120th Congress prepares to convene. Over the past year, Beijing has treated dialogue with the United States as a means of managing risk and buying time while it continues to pursue advantage. Channels such as the new AI incident mechanism may serve U.S. interests by reducing the risk of miscalculation, but the United States cannot allow stability at the leader level to delay the policies needed to compete with and counter the PRC. China's leadership continues to plan against long-term milestones, including the PLA's 2027 readiness goal and the targets set out in the 15th Five-Year Plan, and U.S. policy must be sustained over a comparable horizon. It will be incumbent upon the new Congress, working with the Administration, to harden U.S. critical infrastructure against Chinese cyber intrusions, strengthen deterrence in the Indo-Pacific alongside allies and partners, give U.S. agencies the authorities and resources to wield economic statecraft effectively, and protect the U.S. innovation base from exploitation. Efforts to counter Beijing have long drawn support across party lines and across Administrations, and that consensus will be essential in the years ahead. This Report continues the Commission's work of identifying gaps and shortcomings in U.S. policy and providing recommendations to Congress to address them. ■

THE COMMISSION'S 2026 **KEY RECOMMENDATIONS**

The Commission highlights 10 of its 30 recommendations to Congress below. The complete list of recommendations appears on page 44.

I. Data are a strategic asset that can drive scientific discovery, economic growth, and national security, but their value depends on the ability to organize, protect, and use them effectively. The United States needs a coordinated framework that makes data more accessible for legitimate uses, gives Americans control over their personal data, and prevents exploitation by China and other adversaries. An American Data Initiative would advance these goals while providing Americans meaningful control over their personal data.

Congress should establish an American Data Initiative to put American data to work as a source of national power, while preserving decentralized ownership, giving Americans control over their own data, and keeping their data out of the hands of China and other adversaries. Congress should:

Organize Federal Data

- Make the Administrator of General Services the Federal Chief Data Officer, with binding standards authority over all agencies and every agency Chief Data Officer appointed by and reporting to the Administrator, after consultation with the agency head.
- Direct the Administrator to govern all federal data by sensitivity and value, including in aggregate, and to make Data.gov the catalog of all federal data, open by default, with registered access for non-public data.
- Direct the Administrator to establish sectoral data foundries that produce AI-ready datasets, beginning with biology and embodied AI.
- Require the Administrator's approval of agency data budgets and bar funding for noncompliant data systems.
- Apply the confidentiality protections of Title 13 to personal data shared through the Initiative and record every access to non-public federal data in a tamper-proof log.
- Give the Government Accountability Office continuous access to those logs and authority to review any access to personal data and require an annual report to Congress with agency scorecards and privacy and civil liberties compliance audited by the Government Accountability Office.

Put Data on the Balance Sheet

- Make it U.S. policy that data held by federal agencies and U.S. businesses are an asset recognized on the balance sheet.
- Direct the U.S. Securities and Exchange Commission to require the Financial Accounting Standards Board to set standards for recognizing data as an asset within two years.
- Direct the Federal Accounting Standards Advisory Board to set comparable standards for federal agencies.
- Direct the Public Company Accounting Oversight Board to set matching audit standards.
- Direct the federal banking regulators to exclude data assets from regulatory capital.
- Condition the Governmental Accounting Standards Board's federal funding on comparable standards for state and local governments.

Let Americans Decide Who Gets Their Data

- Codify the core prohibitions of the U.S. Department of Justice's Data Security Program, including its bars on giving China and other countries of concern and covered persons access to Americans' bulk sensitive personal data and government-related data and its limits on onward transfer, and leave compliance requirements to regulation.
- Direct the President to designate an appropriate Cabinet or agency official to establish a national opt-in program under which data brokers may not sell, license, or share Americans' personal data unless the consumer has opted in through a single federal portal that brokers must check before any transfer.
- Extend the Protecting Americans' Data from Foreign Adversaries Act to require data brokers, under a common statutory definition that applies throughout the Initiative and includes resellers and other intermediaries, to register with the designated official, hold them liable for transfers made without consent, bar transfers to persons under the jurisdiction of China or another foreign adversary regardless of consent, and make these obligations follow the data through every resale.
- Require data brokers, within two years, to obtain consent for personal data they already hold or delete it.

Bring Data Sales Out of the Shadows

- Define the rights in data that companies, governments, and consenting individuals can buy, sell, and license.
- Direct the designated official to register and supervise data exchanges, require data brokers, within two years, to sell personal data only through registered exchanges, and require exchanges to verify data provenance and consumer consent, screen buyers for ties to China and other foreign adversaries, including beneficial ownership and intended use, keep auditable records of every transfer, bar unauthorized resale and improper data combination, bar onward transfers to third countries without equivalent controls, meet security standards, and bar participants under foreign-adversary jurisdiction.
- Direct the Secretary of Commerce to open U.S. data exchanges to participants from allied and partner countries whose governments adopt equivalent consent, provenance, and foreign-adversary screening rules and extend reciprocal access to U.S. participants.

II. The Federal Government has spent years building a wall against risky suppliers in strategic sectors. It now needs a purchasing strategy that makes trusted pharmaceutical production commercially viable. The central obstacle is commercial: manufacturers cannot justify investing in alternative sources of active pharmaceutical ingredients (APIs) and key starting materials (KSMs) without confidence that buyers will continue purchasing from them even when cheaper Chinese supply is available.

To break China's leverage over the supply of essential medicines, Congress should establish a Comprehensive Critical Drug Diversification (C2D2) program built around U.S.-India cooperation. The program should:

- Establish a pharmaceutical supply chain early warning mechanism for a list of essential medicines to identify APIs, KSMs, and critical intermediates and their production sites; identify single-country and single-facility dependencies; flag emerging disruptions; and direct purchasing and investment toward gaps.
- Authorize the U.S. Department of Health and Human Services to establish a Federal Trusted Demand Program, including multiyear commitments for essential medicines made with qualifying U.S. or trusted partner APIs and KSMs. The U.S. government should buy finished medicines it needs while making verified sourcing of critical inputs a condition for participation. The U.S. government should also ensure consistent purchase pricing across agencies. The program should:
  - Coordinate how participating agencies verify suppliers and the origins of their critical inputs, including subpoena authority to demand documentation;
  - Have the ability to make multi-year purchase commitments for essential medicines; and
  - Direct the U.S. government to work with providers to address cost disparities of buying medicines under long-term contracts.
- Include an initiative to support public and private investment in API and KSM production in India. For APIs, producers should be mandated to prove minimal and declining reliance on Chinese KSMs to receive the funding. The initiative should, to the maximum extent practicable, require matching funds from India and coordination with Indian producers to withstand predatory Chinese pricing.

III. The growing proliferation and adoption of Chinese open-weight artificial intelligence (AI) models in the United States carries national security implications for sensitive data, cybersecurity, and dependence on Chinese technology. Uncertainty about how these models behave in sensitive applications, what vulnerabilities they may introduce, and whether safeguards can adequately mitigate those risks warrants greater federal scrutiny. Congress should require enforceable protections for sensitive applications before these models become embedded in critical systems and costly to replace.

Congress should require the Secretary of Commerce, through the Office of Information and Communications Technology and Services (OICTS), in coordination with the Center for Advancing Innovation and Standards for Super Intelligence (CAISSI) and relevant federal agencies, to:

- Restrict deployment in sensitive applications unless safeguards are demonstrated. Within 180 days, identify sensitive uses—including systems controlling critical infrastructure, performing national security functions, or processing bulk sensitive personal data—and prohibit new deployment of covered models in those uses absent a time-limited authorization based on independently evaluated safeguards. Authorizations should address the model, its deployment environment, and its access to data, networks, and tools.
- Require identification and mitigation of existing exposure. Direct federal agencies and covered operators in designated sensitive sectors to inventory existing deployments and implement enforceable mitigation or replacement plans within deadlines established by the Secretary.
- Establish continuing security obligations. Require independent security testing, reporting of significant security incidents, reassessment following material modifications, and verification of compliance. Direct the Secretary to restrict or prohibit the

commercial provision or deployment of designated models where identified risks cannot be adequately mitigated.

- Reduce strategic dependence. Require providers serving designated sensitive applications to maintain documented capabilities to replace covered models and migrate affected systems and data to alternatives meeting federal security requirements.

Within 180 days, the Secretary should also complete a consolidated assessment, building on existing federal evaluations, the National Telecommunications and Information Administration's (NTIA) open-model assessment, and federal supply-chain restrictions. The assessment should distinguish risks inherent in model weights from those arising from hosting, software, updates, and system integration; identify gaps in testing and verification; and inform subsequent requirements without delaying initial implementation.

Congress should authorize and appropriate funding, information-gathering and enforcement authorities, and penalties for noncompliance. The legislation should provide narrowly tailored exceptions for security research and authorized national security activities and require annual reporting to Congress on deployment exposure, compliance, mitigation effectiveness, and remaining dependencies.

IV. The People's Republic of China's (PRC) aggressive actions to reshape the Western Pacific and force unification with Taiwan are intensifying. Yet much U.S. and allied contingency planning focuses on large-scale invasion scenarios rather than coercion below the threshold of war. The United States needs a coordinated playbook with allies and partners for responding to a range of coercive gray zone activities by the PRC in the Indo-Pacific, specifically concerning Taiwan.

Congress should:

- Direct the National Security Advisor to develop a common playbook with allies and partners calibrated to counter multi-domain day-to-day PRC coercion. Departments and agencies involved in executing the playbook should develop tiger teams to address U.S. actions and coalition/allied actions under each area of responsibility. That playbook should provide a unified framework for participating nations to:
  - Share situational awareness and arrange pre-coordinated responses;
  - Counter disinformation and lawfare;
  - Expand combined coast guard operations with Taiwan and regional partners, including through multilateral initiatives; and
  - Support resistance against economic coercion.
- Amend and extend the Taiwan Enhanced Resilience Act to establish a Taiwan Democratic Resilience Initiative led by the U.S. Department of State, implemented through the American Institute in Taiwan in coordination with the Office of the Director of National Intelligence and other appropriate departments and agencies.
  - The Initiative should strengthen U.S.-Taiwan cooperation to support the resiliency of Taiwan's civil society and counter PRC united front activities, election interference, and disinformation campaigns. It should also include information sharing with U.S. allies and partners.
- Direct the National Security Advisor to lead an interagency process to develop a whole of government strategy for deterring, preparing for, and responding to coercive actions by the PRC against Taiwan that are intended to rapidly or substantially alter the status quo, but that fall below the threshold of a large-scale invasion or armed conflict.
  - It should include an assessment of contingency scenarios and for each, provide an assessment of indicators and warnings, likely PRC objectives, decision points, escalation risks, potential effects on Taiwan's access to critical goods and services, and options for coordinated actions with allies and partners.

V. As the 14th Dalai Lama advances in age, China is preparing to turn his succession into an international contest over legitimacy and will likely use coercive tools to shape its outcome. India, which hosts the Dalai Lama and the Tibetan government-in-exile and shares a longstanding disputed border with China, is the center of gravity in this dispute.

Congress should make it the policy of the United States that the Gaden Phodrang Trust is the sole legitimate authority to identify and recognize the successor to the 14th Dalai Lama and that the United States will not recognize any successor selected or installed by the Government of the People's Republic of China. To carry out this policy and ensure U.S. government readiness for the Dalai Lama's succession, Congress should direct the Secretary of State to:

- Lead an internal interagency tabletop exercise on succession scenarios, with participation by the National Security Advisor, the Director of National Intelligence, and the Secretary of Defense, and brief the appropriate congressional committees on its findings within 180 days.
- Establish a senior-level channel with the Government of India for succession contingency planning, including intelligence sharing on Chinese influence operations, and report to the appropriate congressional committees on its status within 180 days.
- Conduct Track 1.5 and Track 2 dialogues and tabletop exercises with Indian counterparts on the political and security implications of succession scenarios.

- Coordinate with allies and partners on a diplomatic response that denies international legitimacy to any successor selected by the People's Republic of China.
- Counter succession-related influence operations by strengthening the Central Tibetan Administration's cybersecurity and resilience against China's cyber and artificial intelligence (AI)-enabled disinformation campaigns.

Congress should provide authorizations and appropriations to carry out these activities.

VI. The Commission reaffirms its 2025 recommendation on post-quantum cryptography. Post-quantum risk is coming faster than the government is acting, and the federal response does not yet match the threat. China is investing heavily in quantum computing and has demonstrated sustained, large-scale collection against U.S. government networks. What Beijing steals encrypted today, it can read once a cryptographically relevant quantum computer exists. That same capability would also allow adversaries to forge the digital signatures that authenticate federal software, firmware, and certificates. The U.S. Government Accountability Office reports that agencies are only beginning migration, citing gaps in expertise, inventories, funding, and testing plans. At this pace, the government will miss its own 2030 target for critical systems. The government needs to treat this with far greater urgency.

Congress should:

- Require by statute that federal agencies migrate high-value assets, Federal Information Security Modernization Act (FISMA) high-impact systems, and public key infrastructure—including root certificate authorities and code- and firmware-signing systems—to National Institute of Standards and Technology (NIST)-approved post-quantum cryptography within 24 months of enactment. The statute should also set an accelerated, binding schedule for all remaining unclassified systems.
- Establish a dedicated post-quantum migration appropriation, separate from agency cybersecurity budgets, based on agency cost estimates certified by the Office of Management and Budget.
- Fund NIST's Cryptographic Module Validation Program and Cryptographic Algorithm Validation Program at levels sufficient to reduce validation wait times for post-quantum products.
- Require agency heads to certify progress to Congress every six months, with signed waivers for any missed milestone.
- Make crypto-agility and vendor post-quantum roadmaps conditions of federal information technology procurement.

VII. Americans should know when the government services they receive and the commercial products they use rely on AI models developed by Chinese companies. Clear disclosure would help consumers, businesses, and investors assess potential risks to data security, privacy, service reliability, and national security.

Congress should make it U.S. policy that Americans know when governments and businesses rely on AI models developed by Chinese companies. Congress should:

- Require federal agencies, and any state or local government or other entity that receives federal funds or federal tax credits, to disclose any use of AI models developed by an entity headquartered in, or organized under the laws of China, or owned or controlled by such an entity, including models fine-tuned on or derived from them, wherever they are hosted. Disclosure should appear in clear language on their public-facing platforms and in their filings with the federal government.
- Require businesses that use such models in any part of a product or service offered in the United States to consumers or other businesses to disclose that use clearly on their websites and in product documentation and treat failure to disclose as an unfair or deceptive act or practice enforceable by the Federal Trade Commission.
- Require reporting companies, as part of quarterly and annual disclosure filings with the U.S. Securities and Exchange Commission, to disclose as a material business risk the extent of their use of such models.

VIII. Sustaining U.S. leadership in AI requires reliable access to advanced chips and the manufacturing capacity needed to produce them. Exports to China should not come at the expense of capacity needed to support U.S. AI development and deployment. Requiring auditable exporter certifications would help ensure that export decisions account for these constraints and protect U.S. access to critical capacity.

Congress should ensure that AI chip exports to China do not divert capacity from the U.S. market, including by amending the Export Control Reform Act of 2018 (ECRA) to condition exports, reexports, or in-country transfers of advanced AI chips to China on exporter certification that they will not divert advanced semiconductor manufacturing or AI capacity from the U.S. market. The legislation should:

- Cover upstream capacity, including advanced-node wafer fabrication, high-bandwidth memory, and advanced packaging —not finished-chip inventory alone;
- Require auditable capacity-allocation data submitted to the Bureau of Industry and Security, subject to ECRA recordkeeping and enforcement provisions, including criminal penalties for false certification;

- Require the Bureau of Industry and Security to report annually to the committees of jurisdiction on certifications, validation methods, and exports coinciding with unmet U.S. or allied demand for equivalent capacity; and
- Prohibit regulatory waivers or narrowing of the requirement without an affirmative national security determination transmitted to Congress for a 30-day review period.

IX. The Submarine Cable Act of 1888 only allows the United States to prosecute damage to subsea cables that occurs within U.S. territorial waters (i.e., within 12 nautical miles of its coastline) or damage caused by U.S.-flagged vessels wherever they operate. Current law limits the United States' ability to address other intentional damage to subsea cables landing in the United States or owned by U.S. entities. The United States must also address its limited repair ship capacity, which has led regulators to allow foreign adversaries to maintain U.S. cables that connect to the United States from a third country. This means provisions that would expand a trusted repair fleet and would ensure reinsurance for cable repair surge capacity during a crisis.

To address adversarial attacks on critical U.S. telecommunications infrastructure in international waters, Congress should:

- Amend the Submarine Cable Act to expand jurisdiction to prosecute acts of intentional sabotage against any critical undersea infrastructure landing in the United States or having any ownership stakes from U.S. entities.
- Strengthen undersea cable repair capacity by:
  - Barring the use of foreign adversaries' repair ships on U.S. cables and directing regulators to take associated action;
  - In a manner consistent with current law, establishing a Pacific Allied Cable Repair Fleet, under which the Secretary of Transportation may enter operating agreements with qualified cable vessels flagged in the United States, and, where necessary, Japan, South Korea, and Taiwan; and
  - Directing the Secretary of Transportation to provide insurance or reinsurance against war risks for foreign vessels engaged in cable installation and repair, in coordination with allied countries when possible.

X. For over two decades, China has quietly pursued the development of domestic commodities exchanges, and expanded its production and processing of core commodities, becoming a key market maker in many segments and sectors. China is actively working to exert greater influence over global commodities markets with the aim of advantaging its domestic manufacturers and insulating itself against U.S. sanctions. To this end, China is pursuing numerous policies to expand its leverage, growing its domestic commodity exchanges, and opening more "in China for China" commodities trading to foreign participants. In recent years, China established the China Mineral Resources Group and other state instruments to consolidate purchasing of key commodities and has begun leveraging its position as a major buyer in physical markets to compel producers to use its preferred benchmarks and, in some cases, transact in RMB. China is building parallel systems that, absent action, may, over time, reshape the global landscape.

Congress should direct the U.S. Commodity Futures Trading Commission (CFTC) to monitor Chinese engagement and influence in commodities exchanges and warehousing and provide an annual report to Congress on activity, strategic risks, and efforts to coerce market participants as well as signs of market manipulation. To support this activity, Congress should:

- Expand CFTC foreign market surveillance and provide the CFTC the direction and, as needed, authority to monitor trading activity on Chinese exchanges, including but not limited to the Dalian Commodity Exchange (DCE) and the Shanghai International Energy Exchange (INE), with particular attention to participant concentration, state-owned enterprise positioning, and coordination among state-owned buyers. Current CFTC jurisdictional limits leave this activity unmonitored, and the China Securities Regulatory Commission does not make these data public.
- Direct the CFTC to monitor the development of China's futures markets, in particular for semiconductor, battery, renewable energy, and critical industrial materials. Data on commodity pricing are difficult to obtain, particularly in markets where benchmark usage and settlement terms are embedded in opaque, privately negotiated contracts and are not systematically reported. Thinly traded contracts are susceptible to a risk of biased market data, putting U.S. producers at a disadvantage.
- Require disclosure of U.S. financial institution exposure to Chinese exchanges and other non-CFTC-registered foreign exchanges, as appropriate. Dodd-Frank reporting captures most U.S. derivatives activity on domestic and CFTC-registered foreign exchanges; however, many Chinese exchanges, including the INE, fall outside this framework, and these exchanges have not sought CFTC registration as Foreign Boards of Trade, meaning U.S. firms can trade on them without that activity being systematically captured in CFTC reporting. ■

CHAPTER 1: U.S.-CHINA ECONOMIC AND TRADE RELATIONS

Year in Review

In 2026, China's two-speed economy continues. The country's structural economic weaknesses became more apparent, even as the Chinese Communist Party (CCP) doubled down on its strategy to promote production and innovation in targeted industries and rely on exports to absorb the excess. Rather than address persistent weak domestic demand and deflationary pressures, China allowed its consumption support programs to expire and continues to funnel credit and investment toward its oversaturated manufacturing sector. The conflict in Iran has introduced a cyclical element to these challenges as global energy supplies tighten, raising costs for China's manufacturers and leading to economic hardship for many of China's trade partners.

China's export of its excess production means it is well on its way to a trade surplus of over $1 trillion for the second year in a row. This "China Shock 2.0"—a flood of low-cost exports—is hurting economies all over the world that fail to put up barriers to China's market distortions as their manufacturing sectors are undercut by cheaper products. Many of China's trade partners have introduced more measures to protect domestic manufacturing sectors, including traditional WTO remedies as well as non-tariff barriers. At the same time, China has sought to use concerns about U.S. trade policy to enhance its market access, ironically, claiming to be a more reliable trading partner that supports the rules-based trading system.

Instead of addressing these growing issues, China's 15th Five-Year Plan released in 2026 showcases its continued focus on technological dominance. Beijing hopes its efforts to dominate technology supply chains and innovate at the frontier—combined with its own de-risking measures—will allow it to weather the broader economic slowdown, achieve self-sufficiency, and enhance its geopolitical power. China has also deepened and expanded its toolkit to exert economic leverage on global markets as well as resist foreign sanctions and export controls.

TABLE 1
CHINA'S GROWING ECONOMIC STATECRAFT TOOLKIT PUSHES BACK AGAINST THE UNITED STATES' SUPPLY CHAIN DIVERSIFICATION EFFORTS

Effective Date	Instrument	Authority	Purpose and Key Milestone
March 23, 2025	Anti-Foreign Sanctions Law (AFSL) Implementation Provisions (State Council Decree No. 803)	State Council	Broadens explicit scope of AFSL trigger actions and clarifies countermeasures.
March 31, 2026	Provisions on Industrial and Supply Chain Security (State Council Decree No. 834)	State Council	Unifies a national system for monitoring and responding to threats to supply chains. Targets foreign due diligence and information collecting in China.
April 7, 2026	Regulations on Countering Improper Extraterritorial Jurisdiction by Foreign States (State Council Decree No. 835)	State Council	Targets foreign measures deemed extraterritorial and unjustified. Creates a Malicious Entity List of companies that participate in implementing the foreign measures. First use in May 2026.
June 15, 2026	Regulations on the Implementation of the Mineral Resources Law (State Council Decree No. 839)	State Council	Expands state authority over the granting of mining rights and clarifies process for determining national list of strategic minerals.
July 1, 2026	Regulations on Outbound Investment (State Council Decree No. 837)	State Council	Restricts outflow of technology, services, goods, or other information.

Source: See the full Annual Report for complete table and list of sources.

Key Findings

- China's two-speed economy persisted in 2026. Weak domestic demand and shrinking profit margins weighed on businesses at home, even as General Secretary of the CCP Xi Jinping pressed ahead with efforts to dominate global manufacturing supply chains and advanced technology sectors while strengthening Beijing's ability to exert economic leverage and withstand pressure from abroad.

- China still has not lived up to its repeated promises to spur greater consumption. Continued malaise in the property market has kept domestic demand muted, contributing to excess supply in the manufacturing sector. An estimated 87 percent of Chinese urban households own property; with average home prices having declined 20–25 percent since their peak in 2021, the average Chinese household's wealth has been reduced significantly.

- Weak labor demand and technological displacement are pushing more workers into "flexible" employment in the "gig" economy, leading to lower and less stable earnings, limited career advancement, and weaker social protections. As of 2026, 320 million people worked flexible jobs, including workers from traditionally professional occupations, such as software engineers, financial analysts, and healthcare workers, placing constraints on China's ability to boost consumption.

- Beijing implicitly acknowledged the problem of excess production through its "anti-involution" campaign targeting harmful price competition, as Chinese companies repeatedly slash prices to unload surplus output. The campaign remains limited in 2026, however, and Beijing is unlikely to move more aggressively to curb supply; doing so would undercut exports, a core growth driver, and eliminate many firms' sole pressure release valve, in addition to putting greater pressure on the labor market.

- China Shock 2.0 shows no signs of abating: China's exports accelerated in the first half of 2026 after a record trade surplus in 2025. The resulting flood of exports is hurting manufacturers in developed and developing economies alike, while Beijing has used a range of tactics to forestall a coordinated response.

- Despite the current détente with the United States, China continues to expand its ability to wield supply chain leverage, withstand U.S. and allied sanctions and export controls, and retaliate against foreign measures the CCP deems "unjustifiable" (see Table 1). These efforts are setting up a clash between competing regulatory systems that could leave foreign companies operating in China caught between conflicting demands while raising the costs the United States and its partners must weigh when using economic statecraft.

- The 15th Five-Year Plan confirmed that China remains committed to mobilizing the full weight of the state to advance its technology sector. Beijing treats artificial intelligence (AI) as a general-purpose technology—the connective layer driving other priorities, including biotechnology, robotics, and quantum—believing that mastering these foundational technologies will secure a durable, economy-wide advantage and overcome its economic challenges.

- China continues to face significant compute constraints due to U.S. export controls, yet its frontier AI capabilities have largely kept pace with advances in the United States. Chinese developers are using techniques such as distillation to steal the methods and outputs of top U.S. models to develop capable, lower-cost Chinese alternatives. By releasing these models with open weights and encouraging their adoption abroad, China aims to make its AI systems the global default. U.S. leadership in frontier AI remains real, but China's strategy for spreading its models could make that lead less secure than it appears.

- As China's technologies advance, Beijing is refining its economic toolkit to keep capital, technology, data, and talent at home: screening outbound investment, blocking foreign acquisitions of Chinese firms, restricting AI researchers at frontier labs (and their families) from leaving the country, and limiting the types of foreign investment permitted in its AI companies. ■

CHAPTER 2: U.S.-CHINA SECURITY AND FOREIGN AFFAIRS

Year in Review

Throughout 2026, China used its growing military, technological, economic, and diplomatic power more assertively while seeking to avoid direct confrontation with the United States. Summits between President Donald J. Trump and General Secretary of the CCP Xi Jinping in May and September 2026 reflected this dual-track approach. Beijing embraced "constructive strategic stability" as a framework for managing competition with the United States, even as it continued to strengthen its military capabilities, press territorial claims in the Indo-Pacific, support U.S. adversaries, and expand its influence abroad.

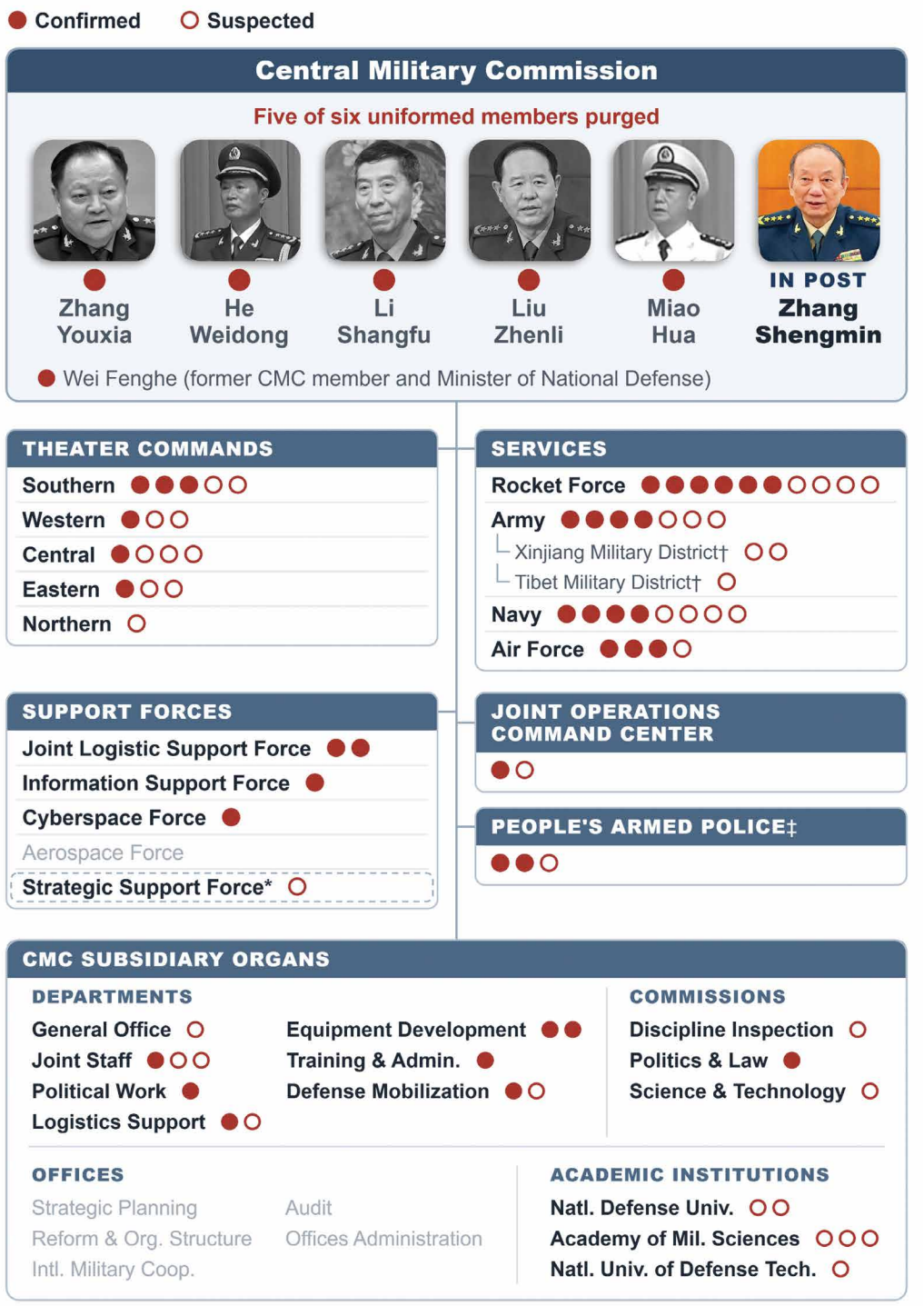
China continued to build the military capabilities needed to shift the regional balance in its favor while pressing its interests across the Indo-Pacific. Despite sweeping purges of the People's Liberation Army's (PLA) senior leadership, military modernization continued, including advances in amphibious warfare, uncrewed and AI-enabled systems, and nuclear forces (see Figure 1). Beijing paired these growing capabilities with a more persistent military and law enforcement presence around Taiwan, increased pressure on Japan, and continued efforts to assert its maritime claims in the South China Sea. China also adjusted the timing and intensity of its activities when confrontation threatened other priorities, underscoring Beijing's effort to advance its regional objectives while limiting the risk of direct conflict.

Beijing used global conflicts to strengthen important partnerships and improve China's international standing while limiting its own exposure to its partners' confrontations with the United States and U.S. allies. China sustained Russia's war effort and Iran's military and economic capacity without becoming directly involved in either conflict. Beijing also expanded engagement with several U.S. allies and partners while portraying itself as a more stable and predictable international actor. China sought to expand BRICS and Shanghai Cooperation Organization (SCO) activities into new areas of security, technology, finance, and governance while expanding strategic infrastructure and security relationships across Africa and Latin America.

China's greater reach did not mean Beijing could always get other countries to follow its lead. Members of BRICS and the SCO resisted or slowed some Chinese-backed initiatives, while governments across the Indo-Pacific pushed back against Chinese pressure. China's expanding security relationships also did not always give Beijing or its partners the ability to shape events in a crisis. These limits did not substantially alter China's direction. Beijing continued to pursue incremental gains, grow its military power, and advance its technology sector, strategic access, and global influence. With two more Trump-Xi meetings expected before year's end, Beijing will likely continue using "constructive strategic stability" to cement its version of the relationship while steadily strengthening China's position.

Beijing will likely continue using "constructive strategic stability" to cement its version of the relationship while steadily strengthening China's position.

FIGURE 1
PURGES OF SENIOR OFFICERS IN THE PLA AFFECT NEARLY EVERY MAJOR ORGANIZATION



Note: This chart shows the known and suspected purges of PLA officers ranked Lieutenant General/Vice Admiral and above between July 2023 and October 2026. Solid circles indicate officially confirmed disciplinary action: expulsion from the CCP, arrest, or removal from post or from China's national legislature or political advisory body for violations of discipline and law. Hollow circles indicate individuals who are missing from public view, reportedly under investigation, or removed or replaced without a stated disciplinary reason. Affiliation reflects the individual's most recent position, which may predate their purge.

* The Strategic Support Force was dissolved in 2024.

† Administered by the PLA Army, operationally subordinate to the Western Theater Command.

‡ The People's Armed Police is a paramilitary force separate from the PLA but answers directly to the CMC.

Source: See the full Annual Report for complete list of sources.

Key Findings

- China accelerated its bid to reshape the international order in 2026. Beijing pursued a coercive but controlled strategy, using its growing military, technological, economic, and diplomatic power to strengthen its position relative to the United States while managing the risk of a destabilizing confrontation. China's actions before and after the Trump-Xi summits demonstrated that its version of "constructive strategic stability" does not mean constraining China's broader competition with the United States.

- Even as Beijing sought to manage its diplomatic relationship with Washington, it continued destabilizing activities aimed at the United States, including cyber operations targeting U.S. critical infrastructure, AI-enhanced influence campaigns aimed at the U.S. public, attempts to co-opt U.S. officials, and transnational repression on U.S. soil.

- Xi Jinping concentrated military authority to a degree not seen since the Mao era through sweeping purges of the PLA's senior leadership, placing greater weight on his personal judgment in decisions over whether and how to use force. Despite the upheaval, PLA modernization continued toward its 2027 readiness milestone for a Taiwan contingency.

- China expanded the scale and sophistication of coercive gray zone activities around Taiwan in 2026 while continuing to build military capabilities for a future conflict. Beijing rehearsed blockade operations, practiced mobilizing civilian fishing fleets, and conducted its first-ever "traffic enforcement operation" in waters east of Taiwan, integrating military, law enforcement, and civilian assets to establish a more persistent presence around the island.

- China remained a critical enabler of Russia's war effort and Iran's military capacity in 2026 while carefully avoiding direct involvement in their conflicts. China facilitated more than 90 percent of Russia's imports of sanctioned technology and supplied Iran with drone components and materials used to make missile fuel while using the growing dependence of both partners to expand its own strategic leverage.

- China's new Ethnic Unity Law extended Beijing's legal claims beyond its borders, creating a statutory basis to target overseas individuals and organizations for activities it deems threatening to "ethnic unity." The provision could create legal and political exposure under Chinese law for U.S. persons and institutions engaged in Taiwan advocacy or Uyghur, Tibetan, and other minority rights work.

- Beijing expanded efforts to build long-term influence and strategic access abroad in 2026. China grew its partnerships, pushed multilateral institutions into new security and governance roles, embedded dual-use infrastructure across Africa and Latin America, and weaponized commercial relationships for political coercion. Beijing also sought to portray itself as a more reliable partner than the United States, but resistance from key partners revealed the limits of its ability to dictate outcomes. ■

Xi Jinping concentrated military authority to a degree not seen since the Mao era through sweeping purges of the PLA's senior leadership.

CHAPTER 3:
CHINA'S OTHER FRONT: INDIA AND THE FUTURE OF U.S. STRATEGY IN THE INDO-PACIFIC

India is one of the few powers outside the U.S. alliance system with the scale to materially affect the long-term competition with China. India is the world's most populous country and largest democracy. It is a nuclear power with one of the world's largest militaries. It shares a 2,100-mile contested border with China and occupies a commanding position along critical sea lanes in the Indian Ocean that carry much of China's energy and trade (see Figure 2). While the Western Pacific remains the principal geographic theater of U.S.-China competition, New Delhi presents Beijing with another strategic challenge both on land and at sea. India's rivalry with China is driven by its own strategic

FIGURE 2
MAP HIGHLIGHTING AREAS OF CONTENTION ALONG THE INDIA-CHINA BORDER



* China does not claim all of the Indian state of Arunachal Pradesh and its claim includes a small portion of the state of Assam. The U.S. Government recognizes Arunachal Pradesh and Assam as part of India.

Source: See the full Annual Report for a complete list of sources. Created for the U.S.-China Economic and Security Review Commission. Names and boundary representation are not necessarily authoritative. There are additional claims/disputed areas that are not highlighted on this map.

interests, not by alignment with Washington. For the United States, a stronger India could contribute to a more favorable balance of power in Asia while providing an important alternative to Chinese manufacturing and supply chains.

China understands this, and it is actively working to suppress India's rise across multiple domains. Beijing is continuing its military buildup, asserting sovereignty claims along the disputed border, deepening military support for Pakistan, and expanding its naval and surveillance presence in the Indian Ocean. China's sharpest tool, however, is economic. Beijing is using its control over critical industrial inputs, technology, and expertise to preserve its manufacturing advantages and make it harder for India to build competing capacity. China has restricted exports of key inputs and products to India to exert economic pressure, recalled engineers and withheld equipment to slow India's electronics manufacturing, slashed pharmaceutical input prices to undercut new Indian plants, and imposed export controls on battery technology to impede the development of India's clean energy industry. More consequential for Washington, in 2025 Beijing began to require Indian firms to certify that certain Chinese-supplied inputs would not be re-exported to the United States. While China suspended this requirement as part of the broader Trump-Xi trade détente, it is a lever that can turn India's dependence on China into a weapon aimed at U.S. supply chains.

India is responding to Chinese pressure while balancing security concerns against its economic development needs. New Delhi is modernizing its military, building domestic manufacturing capacity, restricting Chinese involvement in sensitive sectors, and expanding cooperation with the United States and other partners. However, India recently eased some restrictions on Chinese investment and equipment as the costs of limiting access to Chinese inputs, technology, and expertise have grown. Much of India's industrial expansion still runs on Chinese machinery, components, and technical know-how, and its dependence on Chinese components has deepened even as its de-risking measures multiplied.

These tensions create both opportunities and constraints for the United States. Washington and New Delhi have spent a quarter century building closer ties across defense, technology, and trade, but India will continue to guard its strategic autonomy rather than align automatically with U.S. objectives.

The two governments have established an ambitious foundation for cooperation. A ten-year defense framework, a bilateral trade agreement under negotiation, technology initiatives ranging from semiconductors to biomanufacturing, and a revitalized Quadrilateral Security Dialogue all point toward deeper ties. The legal and institutional architectures needed to support that cooperation have not changed as quickly, however. Export control regimes, procurement rules, and financing tools that were designed for a different era and a different strategic environment limit what these initiatives can deliver. The result is a growing gap between the ambitions of the partnership and what its underlying rules and institutions can deliver.

TABLE 2
INDIA'S IMPORT DEPENDENCY ON CHINA IN SELECTED SECTORS

Product Category	China's Share of Indian Imports	Next-Largest Alternative Supplier
Silicon wafers	97%	Thailand
Lithium-ion batteries	93%	Japan
Antibiotic ingredients	87%	European manufacturers
Active pharmaceutical ingredients	74%	European manufacturers
Solar cells	74%	Indonesia
Electric inverters	62%	Japan
Key starting materials (pharma)	>50%	unknown
Memory chips	46%	South Korea
Industrial machinery	45%	United States

Source: See the full Annual Report for complete list of sources.

Key Findings

- India is one of the few countries with the demographic, economic, military, and geographic scale to significantly affect the long-term balance of power with China. Beijing views India's rise as a strategic challenge and is applying military, economic, maritime, and other forms of pressure to constrain it. India has its own interests driving its rivalry with China and is committed to "strategic autonomy," so closer U.S.-India cooperation will not necessarily translate into alignment with broader U.S. objectives.

- The unresolved border remains the central fault line in China-India relations. The 2020 Galwan Valley clashes marked a major turning point, making India less willing to separate the territorial dispute from its wider relationship with China. Although New Delhi and Beijing have gradually rebuilt ties since late 2024, strategic distrust remains high and India continues to view peace along the border as necessary for broader normalization.

- China's evolving military partnership with Pakistan has made a two-front contingency an increasingly critical concern for India. The May 2025 India-Pakistan conflict demonstrated how China could strengthen Pakistan during a crisis without Beijing entering the fighting directly, adding to India's concerns about how a future conflict with Pakistan could develop.

- China's expanding naval and surveillance presence is beginning to erode India's longstanding strategic advantages in the Indian Ocean and place additional demands on Indian forces. Beijing is building the infrastructure and logistical networks needed to sustain more persistent naval operations while Chinese naval, surveillance, and research vessels operate closer to India and critical sea lanes. China is also beginning to bring its South China Sea playbook to the Indian Ocean, invoking historic rights and renaming undersea features in ways that could lay the groundwork for more assertive activities and potential claims of jurisdiction.

- India's dependence on Chinese manufacturing has become an important source of leverage for Beijing—and a growing vulnerability for the United States (see Table 2). China has restricted industrial inputs, equipment, technology, and expertise to India and required some Indian firms to certify that Chinese-supplied goods would not be re-exported to the United States. Chinese pricing has also undercut new Indian pharmaceutical production, illustrating Beijing's intent to undermine Indian suppliers that can compete with established Chinese producers. These dependencies complicate U.S. efforts to diversify supply chains away from China by shifting production to India.

- India has reduced its exposure to China in some sensitive sectors, but its underlying industrial dependence has continued to grow. New Delhi has restricted Chinese investment, limited Chinese participation in strategic industries, and subsidized domestic manufacturing, yet India's industrial growth has increased demand for Chinese machinery, components, and technical expertise. India's efforts to build domestic supplier networks will require substantial capital, technology, and time, even as it progresses as a global China Plus One hub.

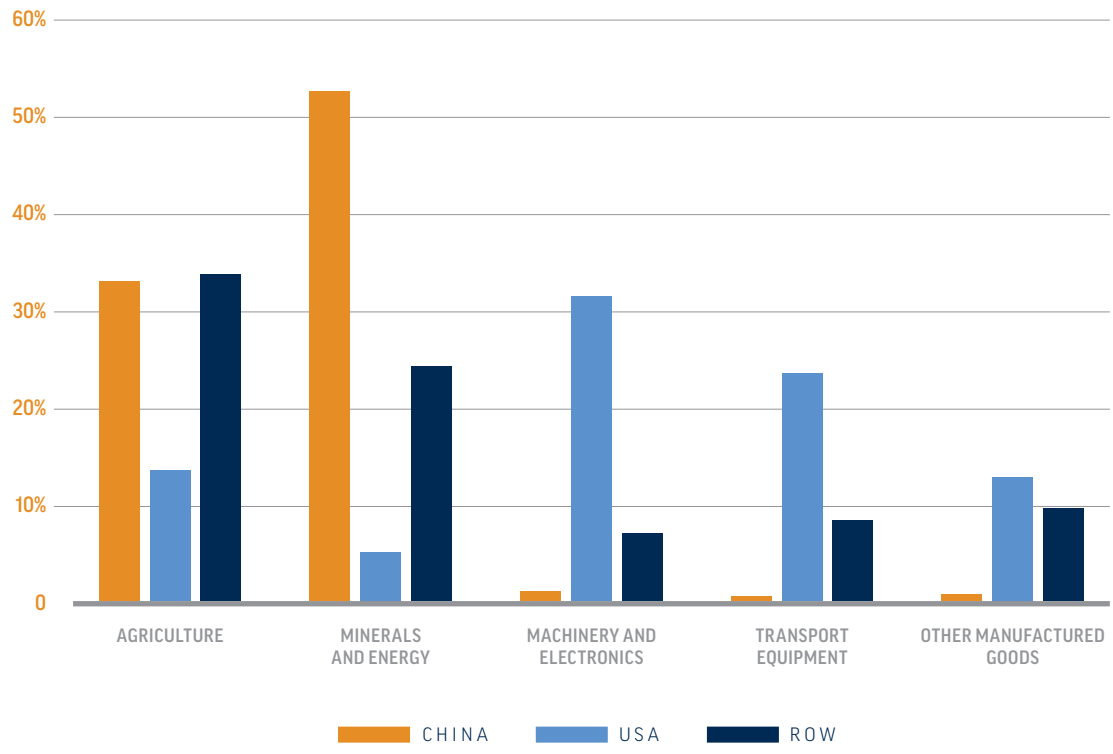
- U.S.-India cooperation has become more ambitious, but many of the rules and institutions governing it remain poorly suited to the partnership's current scope and strategic importance. New defense, technology, supply chain, and maritime initiatives have broadened the partnership, but export controls, procurement requirements, financing constraints, and fragmented bureaucratic processes continue to delay or limit implementation.

China is actively working to suppress India's rise across multiple domains.

CHAPTER 4:
CHINA'S PREDATORY DIPLOMACY IN LATIN AMERICA: BROKEN PROMISES, HARMFUL PRACTICES

For two decades, China has presented itself to Latin America and the Caribbean as a provider of economic opportunity without political conditions, infrastructure without Western constraints, and respect for sovereignty without interference in domestic affairs—yet it has repeatedly failed to deliver. Its economic engagement has reinforced a neocolonial trade pattern in which the region ships raw materials and buys back finished goods (see Figure 3). A "China Shock 2.0" export wave is undercutting local manufacturers and driving the region's trade deficit with China to a record high.

FIGURE 3
SELECT SECTORS' SHARE OF LATIN AMERICA'S EXPORTS TO CHINA, UNITED STATES, AND REST OF WORLD, 2024

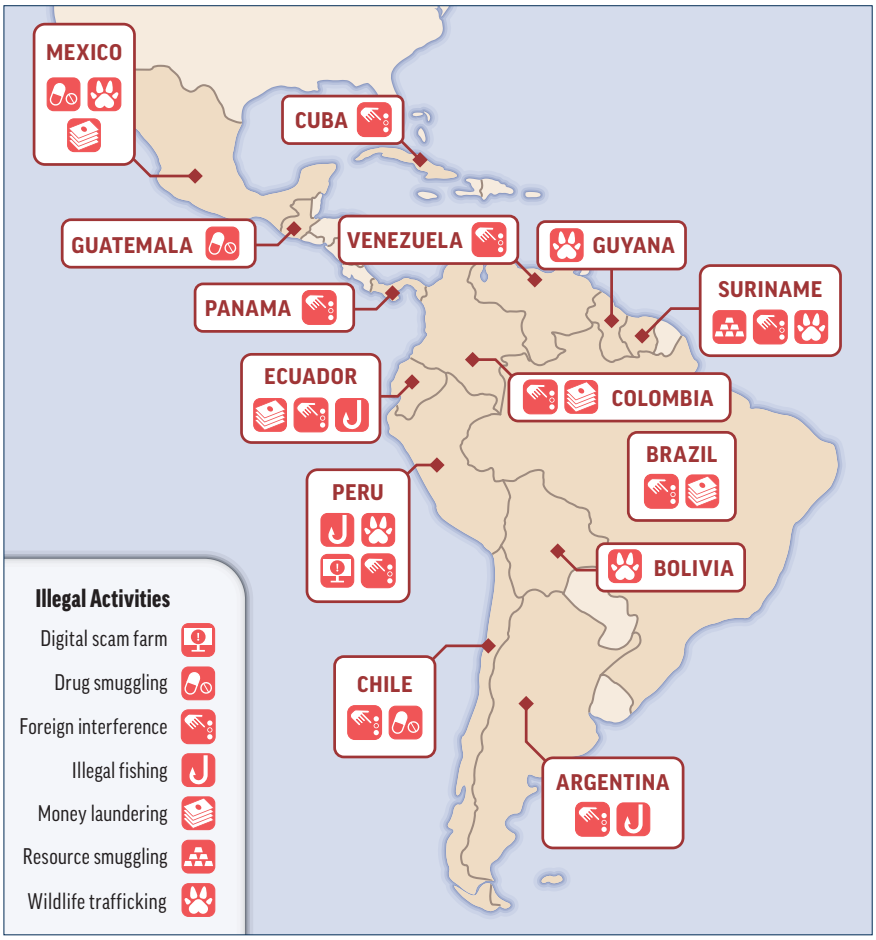


Note: HS codes are grouped as follows: Agriculture (HS 01-24), Minerals and Energy (HS 25-27), Machinery and Electronics (HS 84-85), Transport Equipment (HS 86-89), and Other Manufactured Goods (HS 64-71 and 90-99).
Source: UN Comtrade, accessed June 10, 2026.

Beijing's shift from financing toward ownership and control of ports, power grids, telecommunications, digital, and space infrastructure has converted commercial investment into political leverage and strategic vulnerabilities. Beneath its pledge of noninterference, Beijing works to influence regional institutions through subnational diplomacy, media and diaspora cultivation, coercion relating to Taiwan, and corruption. At the same time, Chinese-linked actors sustain a "Silk Road of Crime" supplying fentanyl precursors, laundering cartel proceeds, driving illicit resource extraction, and supporting other destabilizing illegal activities that Beijing only selectively addresses (see Figure 4).

These trends unfold during a period of both vulnerability and opportunity. China's principal authoritarian partners are weakening: Nicolás Maduro has been removed in Venezuela, Cuba faces an acute crisis, and Nicaragua confronts intensifying U.S. pressure. The United States is contesting Chinese influence and finding receptive audiences among new pro-U.S. leaders moving to diversify trade, restrict Chinese technology, and reclaim strategic assets. Yet two decades of embedded relationships across the region's economies, infrastructure, and institutions have created dependencies that are costly to unwind, and China's successes in emerging sectors such as electric vehicles (EVs) and AI ensure it will remain formidable.

FIGURE 4
CHINA-LINKED CRIMINAL GROUPS ENGAGE IN A WIDE RANGE OF ILLICIT ACTIVITIES ACROSS LATIN AMERICA AND THE CARIBBEAN



Note: Many marks represent allegations or ongoing investigations, not confirmed criminal activity. See the full Annual Report for full descriptions of illegal activities.

Source: Data from Lazarus Consulting. Created for the U.S.-China Economic and Security Review Commission. Names and boundary representation are not necessarily authoritative.

A "China Shock 2.0" export wave is undercutting local manufacturers and driving the region's trade deficit with China to a record high.

Key Findings

- China has inconsistently delivered on promises to advance Latin American development, sovereignty, and security. Instead, its engagement has deepened regional dependence, constrained government autonomy, and aggravated governance challenges.

- The United States is pushing back against some instances of Chinese influence, including by pressuring Beijing's authoritarian partners in Venezuela, Cuba, and Nicaragua. China's muted response, along with growing skepticism among new pro-U.S. leaders, may constrain its near-term agenda. Nevertheless, its subnational networks, critical infrastructure presence, and strength in technologies such as EVs and AI will continue to give it influence in the region.

- The view that China's regional engagement centers on high-profile Belt and Road Initiative (BRI) projects is outdated. Beijing now uses national, subnational, and multilateral channels to create overlapping economic and political dependencies that endure across election cycles.

- Beijing's trade ties have hindered Latin American industrialization and diversification. The region exports raw materials and imports finished goods, while People's Republic of China (PRC) firms dominate higher-value refining. As exports to China have risen, regional manufacturing employment and value added have declined. China Shock 2.0 excess capacity exports threaten further economic harm to the region's manufacturers, contributing to a record $46.9 billion regional trade deficit with Beijing last year and prompting some governments to raise trade barriers.

- China's operational control of ports, telecommunications, energy, and digital networks creates strategic leverage over host governments and potential vulnerabilities for regional sovereignty and U.S. national security.

- Beijing frequently operates below the national level, cultivating governors, mayors, and provincial officials through commercial agreements, sister city partnerships, and Party contacts. These relationships survive elections, provide alternative channels when national governments resist Beijing, and create commitments that are difficult to unwind.

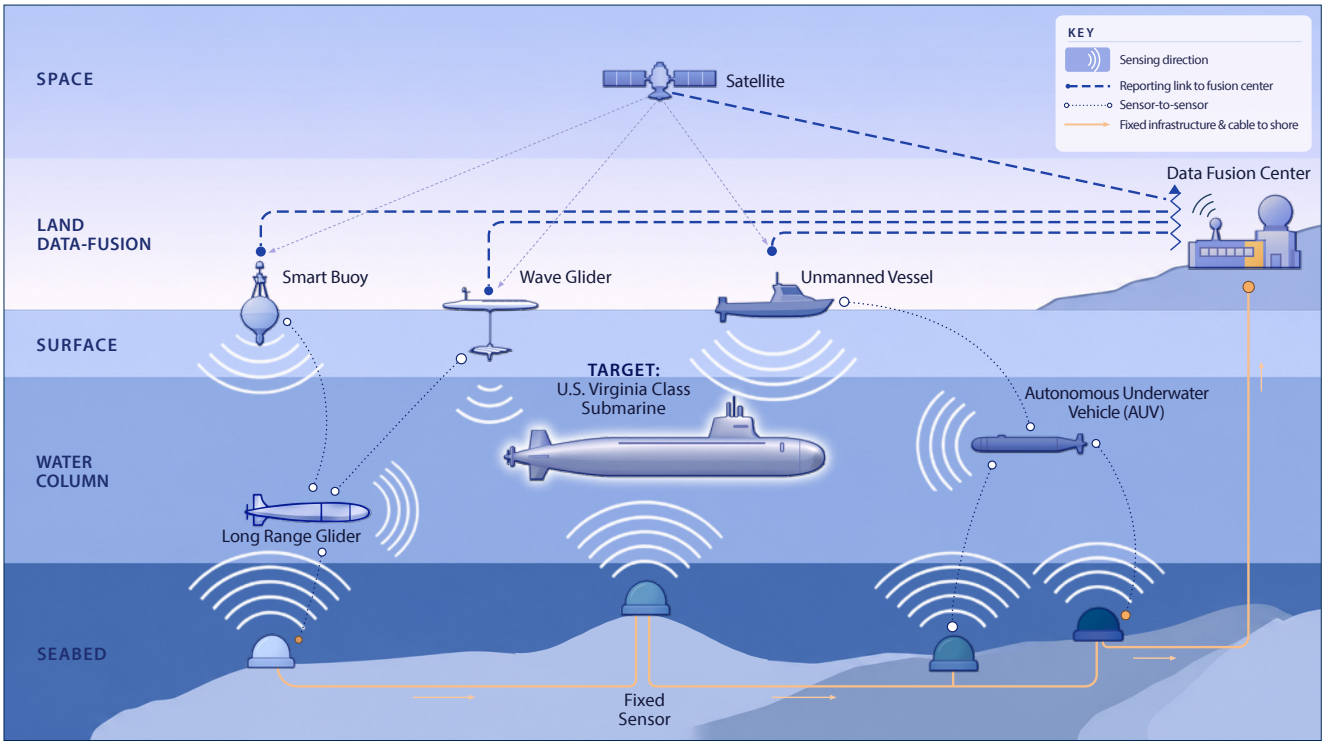
- China's selective law enforcement cooperation leaves gaps that China-linked actors exploit. A "Silk Road of Crime" supplies criminal syndicates with drug precursors, money laundering services, illicit extraction networks, and shell companies—activities Beijing often declines to address. ■

China's operational control of ports, telecommunications, energy, and digital networks creates strategic leverage over host governments and potential vulnerabilities for regional sovereignty and U.S. national security.

CHAPTER 5:
ACTIVE INTERCEPT: CHINA'S EFFORTS TO NARROW U.S. UNDERSEA ADVANTAGE

For decades, the United States has enjoyed a military advantage beneath the sea. China is systematically seeking to erode that advantage. Even as it modernizes and expands its submarine force, Beijing is pursuing multiple means to constrain U.S. submarine operations, particularly by improving its ability to detect them inside the first island chain through a layered sensing architecture and a growing portfolio of autonomous underwater systems (see Figure 5). These efforts could be consequential in a Taiwan contingency, where U.S. submarines would pose a significant threat to PLA forces crossing the Taiwan Strait.

FIGURE 5
CHINA'S "TRANSPARENT OCEAN" CONCEPT INTEGRATES MULTIPLE LAYERS OF UNDERSEA SURVEILLANCE

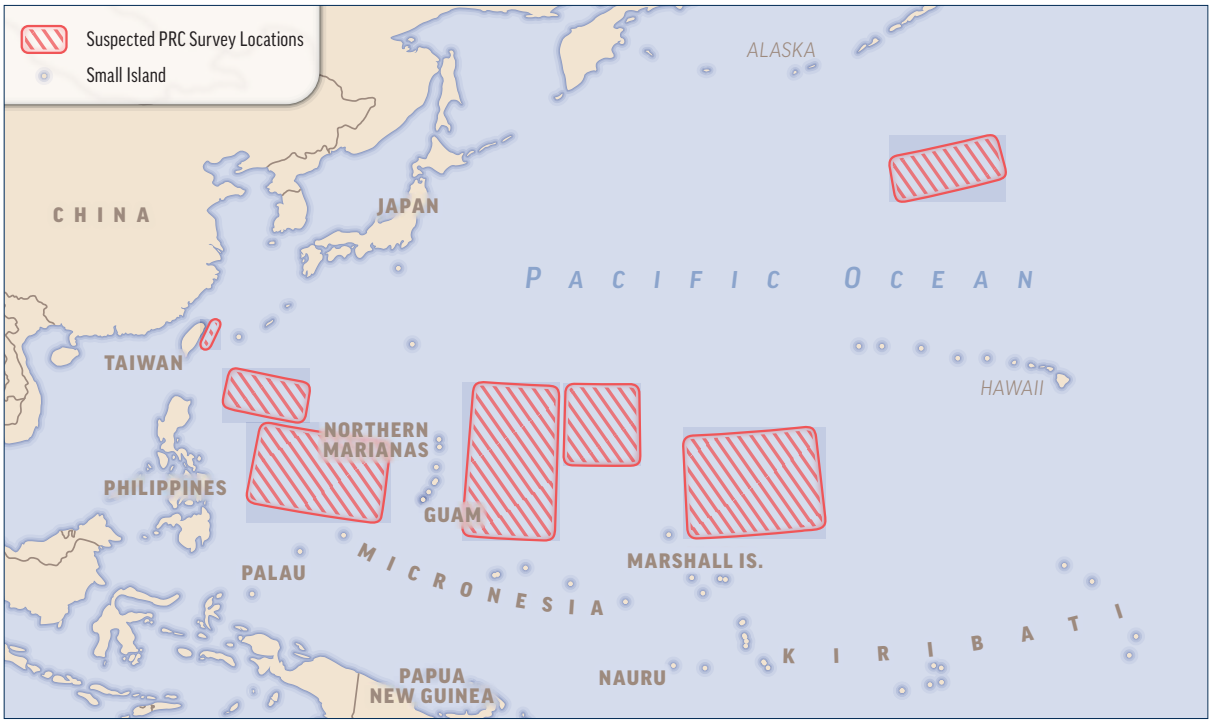


Note: Conceptual illustration. Not to scale.
Source: See the full Annual Report for complete list of sources. Created for the U.S.-China Economic and Security Review Commission.

China treats the undersea domain as a single arena of strategic competition. Beijing is integrating military modernization, scientific research, commercial industries, and emerging technologies into a mutually reinforcing ecosystem that allows capabilities and knowledge developed for one purpose to support others. Military-civil fusion provides institutional channels for scientific and commercial capabilities to support national and defense priorities. Submarine modernization, undersea sensing, autonomous systems, and subsea telecommunications infrastructure provide Beijing multiple ways to improve its ability to understand, operate in, and ultimately contest the undersea environment. Regardless of whether commercial seabed mining becomes economically viable, China's oceanographic research and seabed exploration have produced environmental data, seafloor knowledge, and deep-sea technologies with applications for submarine operations, undersea sensing, and anti-submarine warfare (see Figure 6).

China remains well short of displacing the United States as the dominant undersea military power. Its sensing networks remain fragmented, autonomous systems face substantial technical barriers, and many of its more ambitious concepts remain developmental. However, China does not need to eliminate the U.S. advantage to constrain U.S. operations. Continued gains in sensing, autonomous systems, submarines, and dual-use technologies could narrow that advantage enough to make U.S. operations in the Western Pacific—especially within the first island chain—more difficult, more costly, and more uncertain.

FIGURE 6
MAP OF SELECT CHINESE OCEANOGRAPHIC SURVEY ACTIVITIES IN THE WESTERN PACIFIC



Note: China has also conducted extensive oceanographic surveys in the South China Sea and Indian Ocean as well as maintained ocean sensors off the east coast of Japan. Zhang Tong, "Chinese Team Maps South China Sea Floor with 'Twice the Resolution' of Western Models," *South China Morning Post*, August 31, 2026; Pete McKenzie, "China Is Mapping the Ocean Floor as It Prepares for Submarine Warfare with the US," *Reuters*, March 30, 2026.

Source: See the full Annual Report for complete list of sources. Created for the U.S.-China Economic and Security Review Commission. Names and boundary representation are not necessarily authoritative.

Key Findings

- China is seeking to erode the U.S. undersea advantage through multiple lines of effort that extend well beyond traditional naval modernization. Beijing's investments in submarines, sensing networks, autonomous systems, oceanographic research, subsea infrastructure, and seabed technologies give it several avenues to narrow the U.S. advantage, with institutional links that allow capabilities and knowledge developed in one area to support others.

- China does not need to match the United States submarine-for-submarine to alter the military balance in the Indo-Pacific. China's most immediate undersea objective is not destroying U.S. submarines but rather making them easier to detect. Even intermittent detection of U.S. submarines inside the first island chain could force changes in how they are routed and employed, increase the effort required to preserve stealth, and raise the risks of U.S. intervention in a Taiwan contingency.

- China is developing a layered sensing architecture that could make strategically important waters less permissive for U.S. submarines. Satellites, autonomous systems, seabed sensors, and oceanographic mapping are expanding China's ability to collect undersea data, but integrating these systems into a reliable operational picture remains a major challenge.

- The PLA has a growing portfolio of uncrewed underwater vehicles (UUVs) that conduct a range of missions, but its ability to employ large numbers of them effectively remains unproven. UUVs already support oceanographic collection, sensing, and surveillance, while China is developing systems for mine warfare and other combat missions. If China overcomes persistent communications and coordination challenges, its manufacturing capacity could become an important advantage in fielding autonomous systems at scale.

- China's submarine modernization will place additional demands on U.S. forces charged with preserving the undersea advantage. A larger, quieter, and increasingly nuclear-powered Chinese submarine force will be more difficult to monitor and track, extend the PLA Navy's operational reach, and improve the survivability of China's sea-based nuclear deterrent.

- China's role across the subsea cable industry gives Beijing access to critical infrastructure and strategically important waterways with military and intelligence value. Chinese firms manufacture, own, install, and repair cables supporting global communications, creating opportunities for intelligence collection and maritime surveillance as well as coercion or disruption during a crisis. U.S. actions have constrained Chinese participation in some projects but have not eliminated Beijing's presence across the global cable ecosystem.

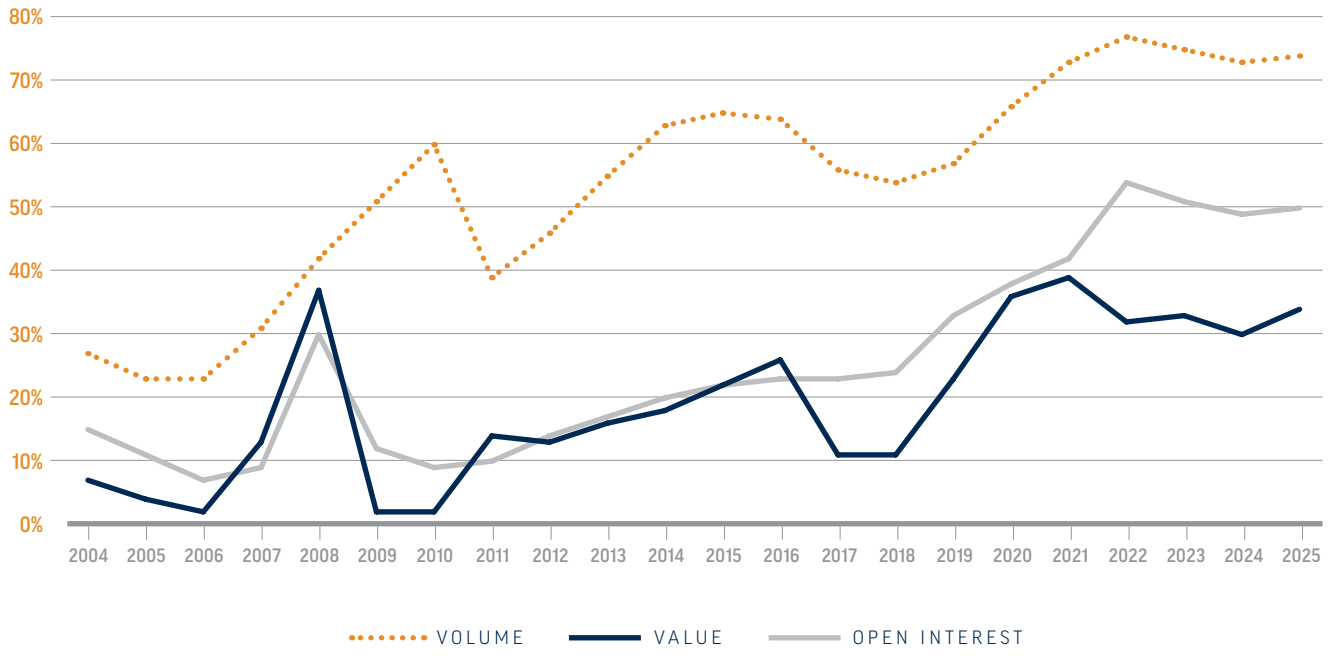
- China is gaining military value from seabed exploration and oceanographic research, driving investments well beyond seabed mining's commercial viability. Seafloor mapping and environmental data can improve understanding of the acoustic environment and inform submarine operations, anti-submarine warfare, and sensor placement, while deep-sea exploration advances relevant robotics and engineering capabilities. China's investments could also position its firms to play a leading role if seabed minerals become commercially important.

China is seeking to erode the U.S. undersea advantage through multiple lines of effort that extend well beyond traditional naval modernization.

CHAPTER 6:
THE PRICE OF EVERYTHING: CHINA'S BID TO RESHAPE GLOBAL COMMODITIES MARKETS

U.S. Ambassador to China David Perdue recently warned that Beijing had "weaponized" its dominant position in critical minerals against the world. China's licensing regime and new regulations could expose individuals trying to diversify supply chains away from China to arrest, criminal prosecution, and asset seizures. While critical minerals are the most urgent chokepoint, China is working to exert greater influence over global commodities markets, pursuing numerous policies that expand its leverage over production and refining, supply chains, and pricing. China has expanded its production and processing of core commodities and become a major force in many segments of agricultural, metals, and energy markets (see Table 3). It has also spent the last three decades developing domestic futures exchanges as a further avenue to exert influence.

FIGURE 7
SHANGHAI FUTURES EXCHANGE, DALIAN COMMODITY EXCHANGE, AND ZHENGZHOU COMMODITY EXCHANGE ANNUAL SHARE OF GLOBAL COMMODITY FUTURES TRADING, 2004–2025



Note: Volume refers to the number of individual transactions where a contract changed hands. Open interest refers to the number of contracts outstanding at a point in time. Notional value reflects the total value of contracts traded in the year. For the purposes of this analysis, commodity options are excluded. Options provide the holder the right, but not the obligation, to buy or sell the product. Trading of options was very limited in China between 2004 and 2015, although it has gained much greater popularity over the last five years.
Source: World Federation of Exchanges, *Statistics Portal*, accessed June 4, 2026.

The United States and its allies in the UK and elsewhere have long dominated global financial markets, governing the process by which prices of key commodities are negotiated. These deep, liquid markets reduce volatility and let buyers and sellers agree on a fair price—not one dictated by the government of a nonmarket economy. China views this status quo as a vulnerability, and its 15th Five-Year Plan signals that it will continue to step up efforts to develop its futures markets and optimize domestic commodity supply chains.

China's influence has already transformed established markets. China has significant reach into the physical infrastructure that transports bulk commodities around the world, vertically integrating mineral extraction, transportation and logistics, refining, and manufacturing of end goods. In 2012, Hong Kong Exchanges and Clearing acquired the London Metal Exchange, which has since approved more Chinese exchange and clearinghouse members, added the renminbi (RMB) as an acceptable currency for margin, and deepened its ties with China's metals industry.

Chinese domestic commodity exchanges are some of the world's largest by trading volume, and they are opening more trading to foreign participants (see Figure 7). At the start of 2020, China allowed foreign investors access to only six futures contracts and no options contracts; today it allows foreign access to over 100 combined. Contracts for lithium traded on the Guangzhou Futures Exchange have achieved global benchmark status over similar contracts introduced by exchanges in the United States and the UK. China has used the China Mineral Resources Group (CMRG), a state-owned consolidated purchaser of iron ore, to compel producers to use its preferred benchmarks and settle more trade in RMB. Even in crude oil, one of the largest and most liquid markets long based on U.S. dollar pricing, China has fostered a regional benchmark for medium sour crude denominated in RMB. This benchmark not only expands China's influence over crude pricing but also could be used to further facilitate sanctions evasion.

As Chinese benchmarks become more widely adopted, China could set the parameters of contracts that global buyers and producers must meet and encourage use of Chinese firms and exchanges. China's success in broader commodities markets has heretofore been hampered by the network effects enjoyed by existing exchanges and hesitation from international producers and consumers to use China's financial markets, which are subject to currency and capital controls, are not protected by the rule of law, and have a high potential for opaque regulatory intervention. However, as a witness noted in written testimony for the Commission, "China's approach is gradual and strategic. It is not attempting to replace existing benchmarks overnight. Instead, it is building parallel systems that may, over time, reshape the global landscape."

TABLE 3
CHINA'S ROLE IN THE GLOBAL MARKET FOR SELECT COMMODITIES

	Share of Global Production/Mining	Share of Global Refining/Smelting	Share of Global Raw Material Imports (2024)
Aluminum	20%	60%	87%
Iron Ore	11%	66%	74%
Soybeans	5%	n/a	65%
Copper	8%	47%	63%
Nickel	3%	31%	61%
Lithium	21%	75%	44%
Oil	5%	18%	24%
Coal	52%	n/a	23%
Natural Gas	6%	n/a	19%
Corn	23%	n/a	8%
Wheat	17%	n/a	6%
Cobalt	1%	76%	4%

Note: For commodities where refining/smelting data are not comparable, consumption data shed light on China's position as a buyer in the global market. For example, China accounts for 56 percent of global coal consumption and 11 percent of natural gas consumption. In agricultural goods, China consumes about 25 percent, 19 percent, and 31 percent of global corn, wheat, and soybeans, respectively. Share of global smelting for iron ore refers to percentage of global pig iron production. Data are the most recent available for each commodity. Units for all commodities' share of production were calculated in metric tons except crude oil and natural gas, which were calculated in barrels per day and terajoules, respectively.

Source: See the full Annual Report for complete list of sources.

Key Findings

- China is moving to translate its physical presence in markets into an alternate network of price benchmarks and futures contracts to give it leverage in key commodities. China has the largest physical presence in commodities markets but has nowhere near commensurate influence or leverage over prices under the current system, partly due to the financialization of commodities markets and the critical role of the U.S. dollar as the dominant currency of exchange.

- China is the world's largest buyer, producer, importer, or refiner of many key commodities. Reliance on imported raw materials led China to take numerous measures to vertically integrate access and operations, including by purchasing the rights to overseas mines, building transport and logistics infrastructure to transport raw materials from overseas to China, and becoming a global leader in refining capacity.

- Beijing is using its physical presence in markets to displace established price benchmarks. In 2022, China consolidated its market power by establishing CMRG to manage purchases of iron ore on behalf of the country's steelmakers. China has since compelled sellers to shift to preferred pricing benchmarks. A state-owned entity, CMRG's political heft has allowed it to issue directives to steel mills to boycott certain suppliers and obtain the support of Chinese government agencies in enhancing its negotiating leverage, including more stringent cargo inspections and higher port storage fees.

- China is leveraging its dominant position in extraction and refining to make rapid progress in expanding domestic commodity futures trading. It is also making progress improving the quality of price signals generated by trading activity. Chinese commodity futures are mostly "in China, for China," a common approach by the CCP to establish an initial market at home before expanding abroad. Still, China has limited influence over global commodity prices, which are largely set by markets, are denominated in U.S. dollars, and are tied to financial exchanges in the United States and other countries.

- To build greater sway in international commodities markets, China is pursuing a multipart strategy that has already influenced pricing and governance:

  ▷ China is leveraging its position in certain newer markets where it has a dominant position in numerous segments of the supply chain, particularly those relating to critical minerals for renewable energy and batteries—for example, lithium. China's dominance of refining and downstream manufacturing limits the capacity for alternative benchmarks to form.

  ▷ China is expanding its network of warehouses for physical delivery in Hong Kong, Shanghai, and abroad to support futures contract settlement. Warehouses linked to commodities exchanges provide the essential infrastructure for storing, managing, and delivering raw materials when futures contracts expire. China's moves increase the appeal of using Chinese futures, expand China's role in price discovery, and grow offshore access to physically delivered Chinese futures.

  ▷ As China shifted its purchases of soybeans from the United States to Latin America, the market is fragmenting between a CME Group exchange and China's competing soybean futures contracts traded on the Dalian Commodity Exchange. U.S. farmers are exposed to further volatility from trade frictions as China substitutes U.S. soybeans for imports from Latin America. China's state-owned agricultural giants are investing in overseas grain storage, port terminals, and soybean crushing capacity that afford them greater insight into pricing dynamics at each stage of production.

  ▷ The conflict in Iran has demonstrated how China has reduced its reliance on global oil markets. Although China's onshore oil benchmark still lags behind major Western benchmarks, it has become an important regional price discovery tool. The existence of an RMB-denominated and locally relevant price discovery tool could allow China's independent refiners to better hedge price risk associated with purchases of sanctioned oil. ■

CHAPTER 7:
COLLECT, STEAL, BUY, FUSE, MONETIZE: HOW CHINA IS TURNING DATA INTO ASSETS AND AMMUNITION

Beijing sees data as a source of national power, not just a commercial asset or a privacy concern. Under Xi Jinping, it has built a state-backed framework for collecting and using data from across society to advance economic, technological, intelligence, and military goals (see Table 4). China's strategy is to maximize the amount and variety of data available to Chinese actors (including but not limited to the Chinese government), improve the state's ability to aggregate and analyze those data, and convert them into economic and strategic advantage. Even seemingly mundane or disconnected information can become more valuable when collected, combined, and analyzed to identify "patterns of life," behaviors, relationships, and anomalies (see Figure 8).

China is building the infrastructure and sector-specific datasets needed to put this strategy into practice. Economically, Beijing has designated data as a factor of production and encouraged local governments and companies to commercialize data within a state-controlled framework. In AI, Beijing is promoting a "data flywheel" in which deployment of AI systems generates real-world data that can improve those systems and support further deployment. In biotechnology, Chinese entities can draw on large

TABLE 4
THE FIVE PILLARS OF CHINA'S DATA GOVERNANCE STRATEGY

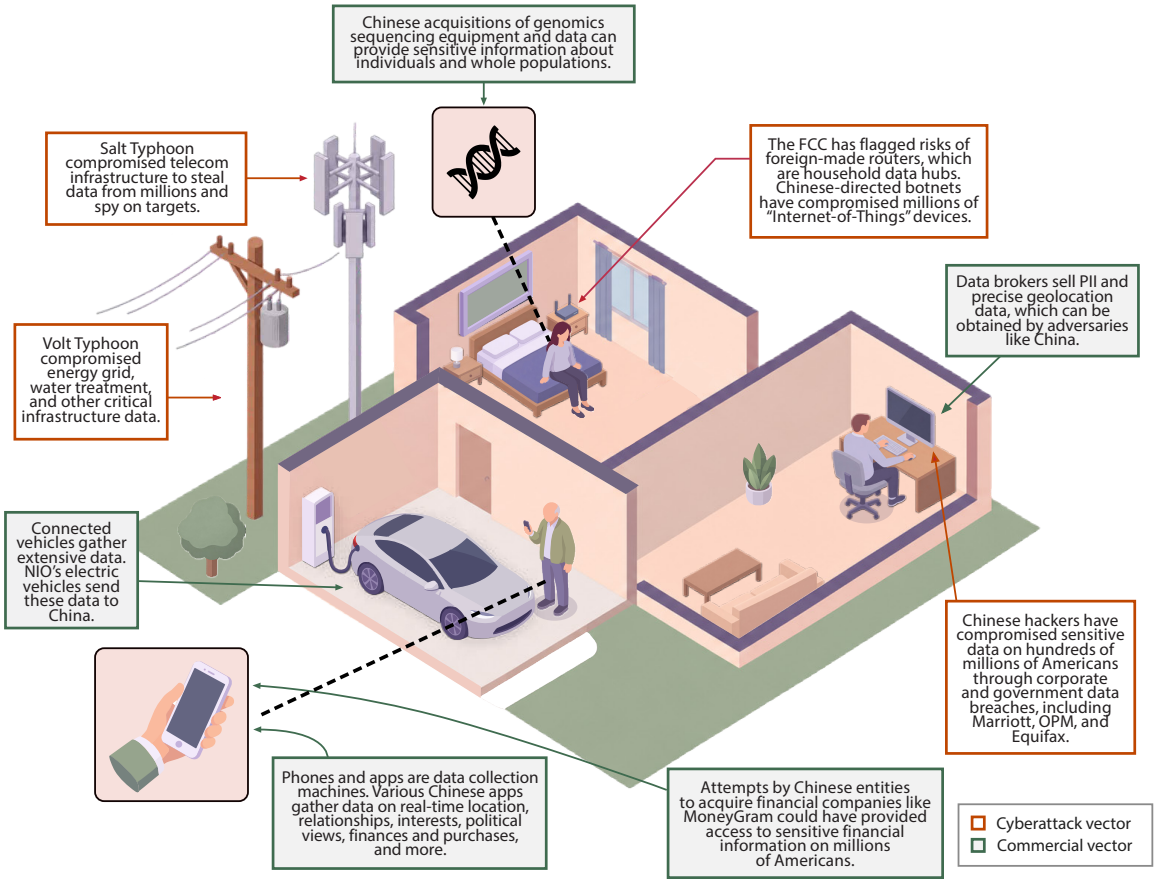
Function	Beijing's Objectives	Key Regulations & Measures
State Access — Ensure the state can obtain data when required	Establish legal authorities to compel companies, organizations, and individuals to cooperate with the state's intelligence and security entities when requested.	National Intelligence Law (2017) Data Security Law (2021)
Data Control — Keep strategically important data within Beijing's regulatory reach	Establish localization, classification, security-review, and cross-border transfer requirements that give authorities greater oversight over sensitive and important data.	Cybersecurity Law (2016, effective 2017) Data Security Law (2021)
Data Protection — Regulate how organizations collect, process, and transfer data	Establish privacy and data security obligations, particularly for personal data and information deemed "sensitive," while regulating overseas transfers.	Personal Information Protection Law (2021) Data Security Law (2021)
Data Mobilization — Turn data into an economic and technological resource	Encourage data sharing, circulation, commercialization, aggregation, and reuse to support the digital economy, AI, industrial upgrading, and government administration.	Factor-of-production policies (2019–20) Twenty Data Articles (2022)
Institutionalization — Build the state capacity to govern and exploit data at scale	Create institutions, infrastructure, standards, markets, and accounting mechanisms to implement the broader data strategy.	National Data Administration (2023) Data exchanges; public data infrastructure; data asset accounting

Source: See the full Annual Report for complete list of sources.

domestic biological datasets and, in some circumstances, foreign repositories, while Chinese regulations restrict foreign access to comparable Chinese data. Data also support China's military, intelligence, and security objectives: the PLA is researching how new datasets can improve equipment, train AI systems, monitor adversaries, identify vulnerabilities, and support operational planning, while Chinese cyber actors have already acquired sensitive personal, technical, and critical infrastructure information with potential intelligence and operational value.

For the United States, the challenge extends beyond protecting individual databases from theft. China can acquire data through both illicit and lawful channels and use them for espionage, coercion, influence operations, technological development, and military planning. U.S. measures have restricted some paths to sensitive American data, but significant vulnerabilities remain, as current U.S. policy largely addresses cybersecurity, privacy, foreign investment, biotechnology, and AI as separate issues. In contrast, Beijing approaches data as a strategic resource that spans across sectors and issues. However, China's ability to translate its data resources into concrete advantages is not assured: commercial data remain fragmented, and high-quality AI training data are scarce. Even so, its drive to collect, aggregate, and exploit data at scale poses an enduring challenge to U.S. competitiveness and national security.

FIGURE 8
CYBERATTACK AND COMMERCIAL VECTORS OF CHINA'S DATA COLLECTION



Source: See the full Annual Report for complete list of sources.

Even seemingly mundane or disconnected information can become more valuable when collected, combined, and analyzed to identify "patterns of life," behaviors, relationships, and anomalies.

Key Findings

- Beijing pursues a state-directed strategy to acquire, consolidate, and exploit data from a vast array of sources, including state surveillance infrastructure, cyber operations, scientific and biomedical sources, and even routine commercial activity, while leveraging AI to fuse disparate datasets into actionable intelligence.

- China acquires data illicitly through state operations as well as via a contracted "hackers-for-hire" ecosystem. This provides it with access to vast troves of information via cyber operations. Yet cyber theft is only one component of a far broader collection apparatus.

- China's legal and institutional architecture ensures state access to data held by any Chinese entity, while cross-border controls allow Beijing to retain high-value Chinese data domestically. Any data a Chinese company collects can be claimed and absorbed by the state, no matter how mundane their commercial purpose.

- In 2020, China became the first country to designate data as a factor of production, alongside land, labor, capital, and technology, a deliberate decision that elevated data to a strategic national asset and an instrument of national power. It is perhaps the only country to have built an end-to-end, state-directed system to control, collect, aggregate, deploy, and exploit data.

- China converts data into power through aggregation. Capabilities refined through its domestic surveillance state—fusing biometric, financial, communications, behavioral, and any other data into predictive profiles—are being applied to foreign targets, with AI accelerating the transformation of disparate datasets into "pattern-of-life" intelligence.

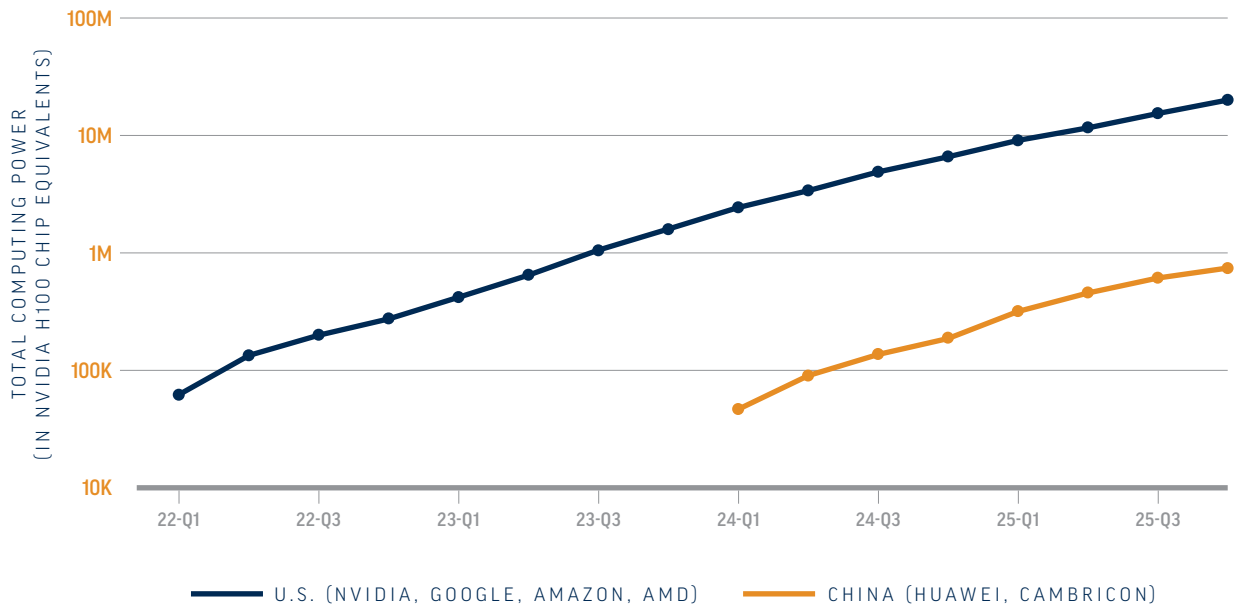
- Beijing is converting its data position into competitive advantage: building a national data infrastructure to power its digital economy; enforcing strategies to generate high-quality AI data by deploying the model in a system that feeds the data back for further iteration; and engineering deliberate asymmetries—most starkly in biotechnology—that maximize access to foreign data while denying reciprocal access to China's data.

- China's data dominance strategy threatens U.S. national security. The aggregation of data on Americans enables espionage, coercion, and influence operations with unprecedented precision; supports pre-positioning campaigns such as Volt Typhoon that collect critical infrastructure data to support "system destruction warfare" in a future conflict; and facilitates the use of stolen technical data to accelerate PLA modernization. Where Washington sees a privacy problem, a cyber problem, and a trade problem, Beijing sees a single resource of national power and has organized its laws, economy, and intelligence apparatus to control it end to end. ■

CHAPTER 8:
SILICON TO SOVEREIGNTY: CHINA'S BID TO CONTROL THE AI STACK FROM WAFER TO WEIGHTS, PART ONE

Competition between the United States and China for leadership in AI extends across the technologies, infrastructure, and applications that underpin the development and deployment of AI systems. Leadership at one layer can create advantages elsewhere in the stack, but weaknesses at one layer can also constrain the performance of the entire system. This makes control over key AI-related technologies, infrastructure, and supply chains a critical issue for U.S. economic and national security. The United States and its allies and partners currently hold substantial advantages in many of the most technically difficult and concentrated segments of this stack. U.S. firms lead in advanced AI chip design and software; Taiwan dominates leading-edge semiconductor fabrication; the Netherlands maintains a monopoly over extreme ultraviolet lithography systems; and South Korean and U.S. firms currently dominate high-bandwidth memory. Together, these advantages have constrained China's

FIGURE 9
CUMULATIVE COMPUTE OVER TIME—U.S. VS. CHINESE ADVANCED CHIP DESIGNERS



Note: Values are summed across designers each quarter—log scale. Quarters shown are calendar-year quarters.
Source: EpochAI.

access to the advanced computing resources required to develop frontier AI systems.

China has pursued technological self-sufficiency for more than two decades, and U.S. technology restrictions since 2019 have increased the challenges—and likely the urgency—of Beijing's localization campaign. Export controls on advanced AI chips, semiconductor manufacturing equipment, and related technologies have disrupted China's access to advanced computing capabilities and slowed the development of its indigenous semiconductor ecosystem, even as Chinese firms continue to make progress. China is simultaneously attempting to engineer around its remaining technological chokepoints while leveraging advantages elsewhere in the AI stack, including China's dominance of critical minerals and materials. These strengths could help China compensate in part for less efficient domestic AI hardware and other technological constraints.

Ultimately, U.S.-China AI competition is unlikely to be determined by dominance at any single layer of the technology stack. Despite constraints on advanced compute, Chinese firms have produced near-frontier models with fewer advanced computing resources, while inexpensive open-weight models have facilitated their rapid international adoption. China could therefore remain dependent on foreign technology at critical portions of the infrastructure layer while gaining influence in global model and application ecosystems. Conversely, U.S. leadership in advanced computing will not automatically translate into broader AI leadership without sufficient energy, networking, and data center infrastructure to deploy these technologies at scale. U.S. and allied export controls can preserve critical technological advantages and slow China's progress, but their strategic value ultimately lies in buying time for the United States to strengthen or solidify its competitiveness across the entire AI technology stack. Part Two of this research will dive deeper on how China is attempting to overcome its own chokepoints across the AI tech stack, including those associated with software, servers, hyperscalers, and energy constraints.

Key Findings

- The United States and allies hold decisive advantages at the top of the stack, and export controls are the principal tool slowing China (see Figure 9). Their continued effectiveness depends on closing loopholes and working closely with allies to prevent their erosion.
- For more than two decades, Beijing has been pursuing self-sufficiency and global competitiveness across the entire semiconductor ecosystem and—more recently—the AI technology stack. U.S. and allied controls did not drive China's indigenization efforts, but they have added urgency in recent years.
- Although China has made some progress in achieving its goals, it has not yet closed the hardest chokepoints—including the most advanced capabilities in logic fabrication, memory, and semiconductor manufacturing equipment, as well as the Nvidia Compute Unified Device Architecture (CUDA) software moat—and likely will not for some time.
- China is investing heavily to engineer around major chokepoints: alternative lithography, advanced packaging, photonics, and an open-weight, lower-compute model strategy. Success is not assured, but U.S. policymakers need to closely follow developments in these areas.
- China's dominance in processing and refining several critical minerals and rare earth elements creates upstream vulnerabilities throughout the AI technology stack for the United States and its allies and partners. Beijing has demonstrated its willingness to leverage this position through export restrictions, raising the risk that it could disrupt U.S. access to materials needed for advanced semiconductors, data center hardware, power systems, and other AI infrastructure during a geopolitical or trade dispute.

CHAPTER 9:
TAIWAN: A CRUCIAL WINDOW FOR A CRITICAL PARTNER

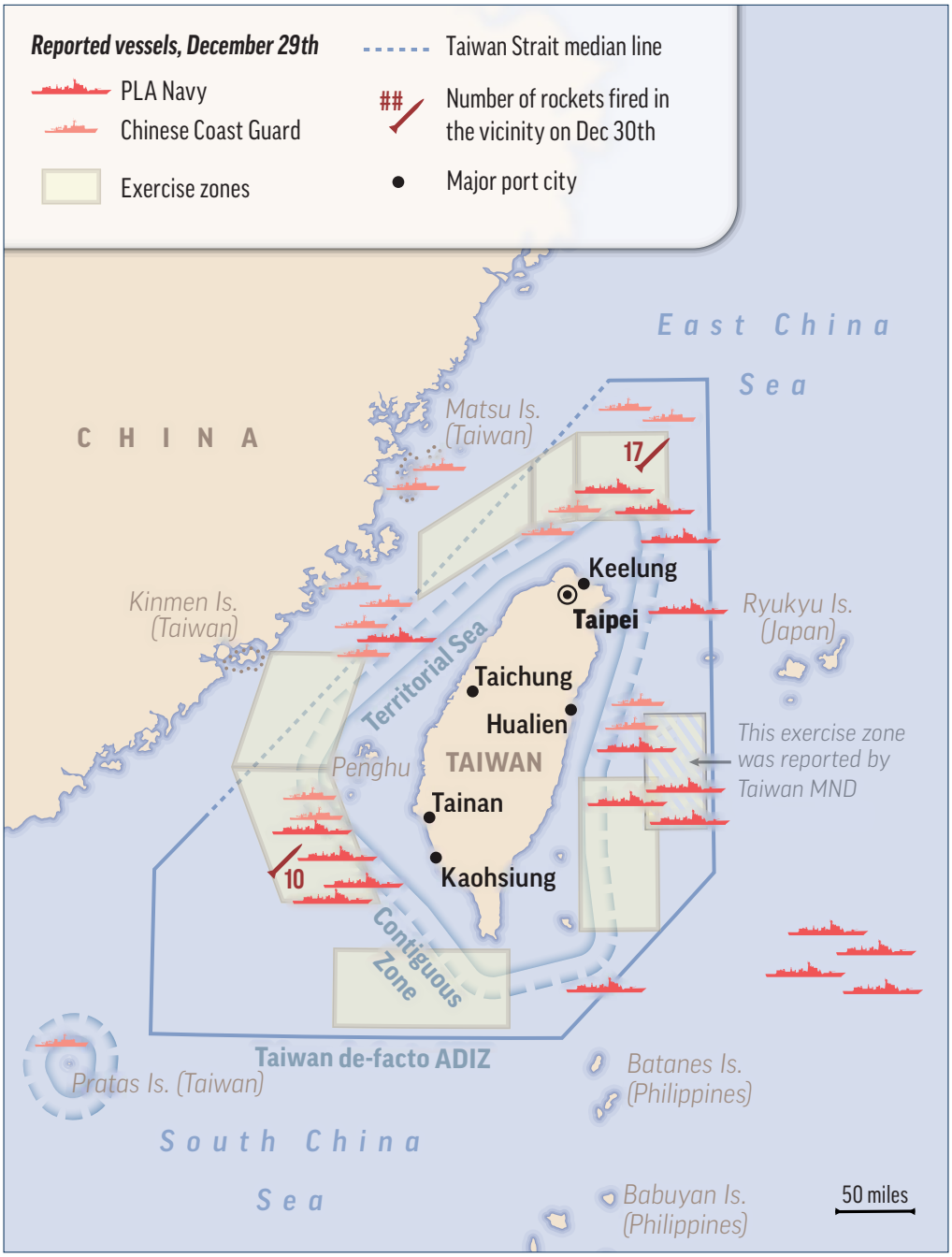
The next 24 months could shape cross-Strait relations for years. Beijing will assess Taiwan's 2026 and 2028 elections to gauge whether coercion and political pressure can move Taiwan toward unification. However, even an outcome the PRC favors may not deliver what it expects. Taiwan's public remains overwhelmingly opposed to political integration with China, limiting how far any elected government can move toward Beijing. Xi Jinping could therefore reach 2028 with greater military capabilities and less confidence that political and economic pressure and other forms of coercion can achieve unification. This realization may increase the risk that China will take more aggressive coercive actions against Taiwan, including imposing a quarantine or blockade.

The stakes for the United States have never been higher. Taiwan is indispensable to the Indo-Pacific balance of power and to U.S. technological leadership and economic security. Taiwan's central geographic location in the first island chain and near key maritime routes constrains China's options and concurrently enhances U.S. access, capabilities, and operational freedom in the Indo-Pacific. In recent years, Taiwan's world-leading semiconductor industry has become foundational to U.S. leadership in advanced technologies, particularly AI. A change in Taiwan's status would alter the military balance in the Western Pacific, test confidence in U.S. alliances, and threaten critical technology supply chains.

Beijing is pursuing its objectives through coercion backed by a credible threat of force (see Figure 10). China is seeking to weaken Taiwan's resistance through military and coast guard activity, cyber and information operations, economic leverage, lawfare, and political influence while building capabilities to blockade or invade the island. Taiwan has responded with increased defense spending, military reforms, investments in resilience, and stronger cooperation with the United States, but significant vulnerabilities remain. Political divisions have slowed defense investments, Taiwan depends heavily on imported energy, and nearly $30 billion in approved U.S. weapons remained undelivered as of August 2026. The near-term challenge is therefore not only to deter invasion but to prepare better for the coercion already happening and likely to escalate—sustained pressure designed to change the status quo without triggering war.

Taiwan is indispensable to the Indo-Pacific balance of power and to U.S. technological leadership and economic security.

FIGURE 10
PLA JUSTICE MISSION-2025 EXERCISE



Note: Ship positions are approximate; placements are adapted from reproductions and adjusted slightly for legibility.
Source: See the full Annual Report for a complete list of sources. Created for the U.S.-China Economic and Security Review Commission. Names and boundary representation are not necessarily authoritative.

Key Findings

- The next 24 months will test Beijing's belief that it can move Taiwan toward unification through coercion and political influence rather than force. This coercion strategy hinges on eventually having a conciliatory government in Taipei, but Taiwan's public overwhelmingly favors the status quo, constraining how far any elected government can move toward Beijing. Even electoral outcomes in 2026 and 2028 that Beijing favors may fail to produce the political movement toward unification it expects. If China concludes its political strategy is failing, Beijing may turn to greater coercion to force progress on its terms, including through imposing a quarantine or blockade.

- Taiwan is a first-order U.S. national security interest. A crisis in the Strait would threaten U.S. military power and economic security simultaneously.

- Taiwan's continued autonomy is critical to the military balance in the Western Pacific, and its security is closely tied to allied confidence in U.S. commitments. Taiwan's geographic location denies the PLA a forward military position between Japan and the Philippines and complicates its access to the Western Pacific. Taiwan's own surveillance, coastal defense, air defense, and maritime capabilities force the PLA to account for threats from the island, while U.S. and allied forces elsewhere along the first island chain further constrain its operations. Chinese control of Taiwan would shift these advantages toward Beijing, extending PLA power in the Western Pacific.

- Taiwan's technology ecosystem is at the foundation of U.S. advantage in AI. Taiwan dominates advanced semiconductor production and supplies critical hardware across the AI stack. U.S. reshoring is building domestic capacity but remains deeply dependent on Taiwan's companies, technology, workforce, and supply chains, making the two economies more integrated rather than making Taiwan dispensable.

- Coercion and military buildup are mutually reinforcing components of Beijing's dual-track strategy rather than alternative paths to unification. Political influence, economic pressure, cyber and information operations, lawfare, and other gray zone activities work to erode Taiwan's will to resist, while the PLA's growing military capabilities make those efforts more credible and preserve Beijing's option to impose unification by force if they fail. U.S. and Taiwan planning remains more heavily oriented toward countering an invasion, leaving both less prepared for the challenge likely to come first.

- China is intensifying its efforts to intimidate and coerce supporters of Taiwan's autonomy, moving beyond symbolic legal threats toward more concrete efforts to punish opposition to Chinese malign influence and to deter support for Taiwan. Over the past year, Beijing introduced new legal authorities, launched criminal investigations, and took public enforcement actions to intimidate a broader range of Taiwan officials, civil society leaders, and public figures, regardless of their location.

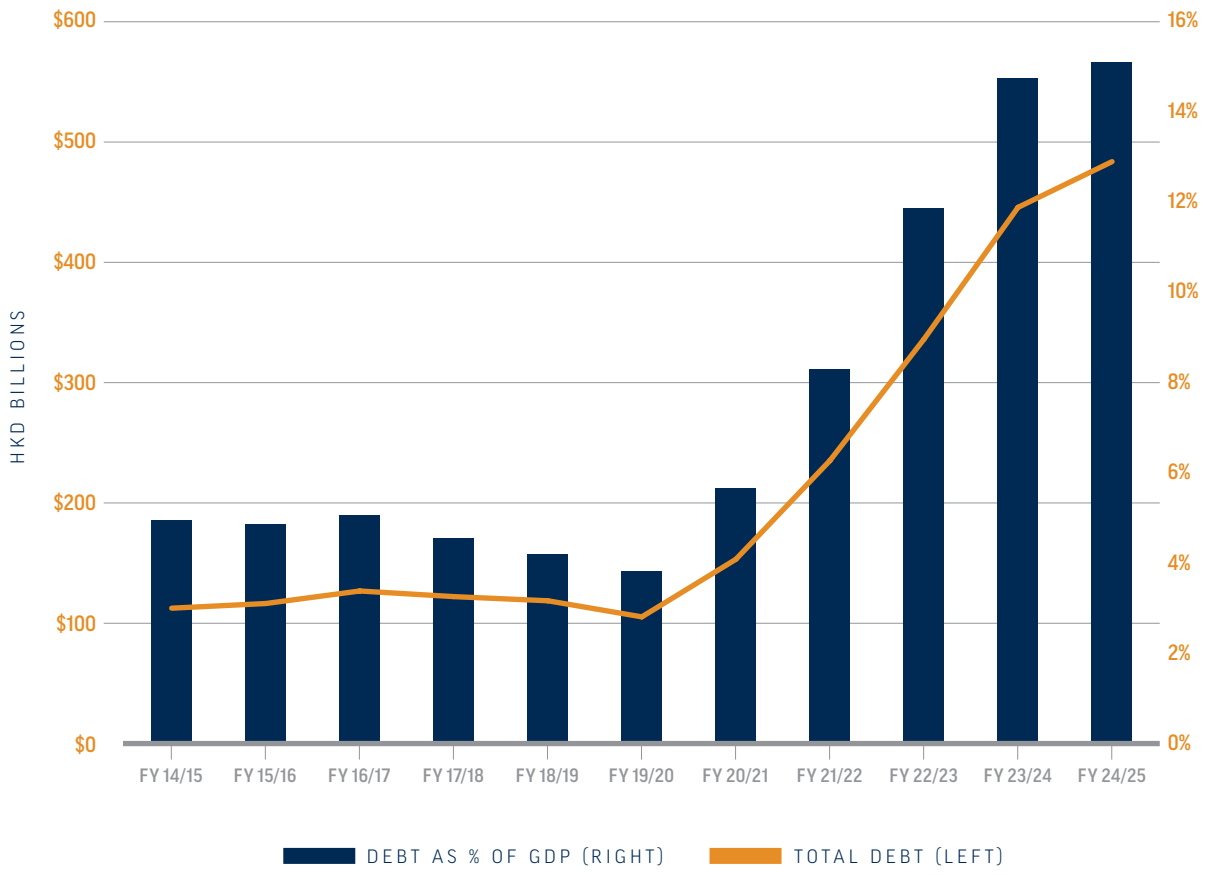
- Taiwan is strengthening its military and national resilience, but domestic political divisions and persistent vulnerabilities threaten to slow progress during a critical period. Taipei is strengthening its asymmetric defenses, civil preparedness, critical infrastructure resilience, and counterintelligence efforts, but legislative gridlock has delayed or reduced investments that could produce near-term capabilities. Taiwan's heavy dependence on imported energy also leaves it particularly vulnerable to the quarantine or blockade scenarios Beijing is increasingly rehearsing.

- Delays in U.S. foreign military sales are hindering Taiwan's ability to field critical military capabilities and weakening deterrence even as Chinese pressure increases. A backlog of undelivered weapons, compounded by delays in finalizing additional arms sales, is pushing needed capabilities further into the future. These challenges slow Taiwan's ability to enhance its capacity to resist Chinese coercion, blockade, or invasion.

CHAPTER 10:
HONG KONG: ENABLER OF CHINA'S GLOBAL FINANCE AND TECHNOLOGY AMBITIONS

Hong Kong's political and judicial systems are now subject to complete CCP control. In 2026, Hong Kong's loyalist legislature passed new rules allowing the chief executive to unilaterally label any criminal matter as a national security case. Those accused of committing national security offenses cannot contest the designation, and there are no elements of civil society left to provide meaningful resistance. With the CCP takeover, the prerequisites for a thriving financial center—rule of law, a fair legal system, and robust market institutions—are at odds with Beijing's

FIGURE 11
HONG KONG GOVERNMENT DEBT FIGURES RISING, 2015–2025



Source: Hong Kong's Census and Statistics Department, via Haver Analytics.

autocratic rule. Yet with the CCP's support, Hong Kong's economy has become a controlled valve for China to achieve its strategic aims vis-à-vis the global trading and investment system.

Despite years of trying, the Mainland's financial markets have not replaced Hong Kong as a conduit to the global financial system. Underdeveloped financial markets and the Party's need to prevent capital outflows limit the ability of cities like Shanghai and Shenzhen to attract offshore capital. As Western markets have become less viable alternatives, Hong Kong has solidified its role as a venue for mainland technology firms to raise foreign capital for global expansion; almost all of Hong Kong's initial public offerings (IPOs) in the first half of 2026 were for mainland companies. Hong Kong is also instrumental to China's efforts to build offshore infrastructure for RMB circulation and investment as it seeks to grow the role of RMB in international financial flows and insulate itself from U.S. sanctions authorities (see Table 5). Hong Kong's active and complex financial system also helps China act as a key enabler of Iran, Russia, and North Korea's sanctions and export control evasion.

The international business community and global financial institutions appear willing to overlook the loss of freedom and rule of law in Hong Kong—and the changing nature of Hong Kong's financial system—as long as the impact to the corporate bottom line remains limited. However, Hong Kong's economy and financial sector are more exposed to geopolitical and economic risks associated with the Mainland. The implementation of top-down economic planning through Hong Kong's first five-year plan and the ongoing subversion of market interests for state priorities set up a fundamental contradiction between what makes a financial center attractive and the purpose China wants Hong Kong to serve.

TABLE 5
HONG KONG IS CRITICAL TO CHINA'S OFFSHORE RMB ECOSYSTEM

Payment Settlement	• Hong Kong is already the largest offshore RMB settlement center, accounting for 75 percent of global offshore RMB settlement transactions as of 2023. • Hong Kong banks participate in the Cross-Border Interbank Payment System (CIPS), China's payments messaging and settlement platform. • In July 2026, Hong Kong Exchanges and Clearing (HKEX), which operates Hong Kong's exchanges, announced it would become a direct participant in CIPS, allowing it to access the platform directly to send and receive payments.
Fixed Income	• Hong Kong's offshore RMB bond issuances, known as dim sum bonds, have grown 60 percent from 2022 with growing liquidity in longer-dated maturities.
Equity Investment	• Hong Kong is exploring an offshore RMB venture capital fund to support the operating needs of mainland firms.
Foreign Exchange	• Hong Kong accounts for more than 30 percent of global trades involving the RMB. USD/RMB trades averaged $274 billion daily turnover in April 2026, the largest of any currency pair in the city.
Trade Finance and Working Capital	• HKMA upsized its RMB Business Facility from RMB 100 billion to RMB 500 billion in 2026, allowing banks to provide greater offshore RMB liquidity to their corporate clients.
Interest Rate Risk Management	• Hong Kong comprised 39 percent of average daily turnover for global RMB interest rate derivatives in April 2025. • HKEX launched the first offshore government bond futures contract, expanding offshore risk management tools for holders of mainland assets.

Source: See the full Annual Report for complete list of sources.

Key Findings

- Beijing's strong support has been the decisive factor behind Hong Kong's financial improvements over the last year. Hong Kong led the world in IPOs in 2025, with a comparable level of activity in the first half of 2026—not as a revived global hub but as a venue of choice for mainland firms in Beijing's priority sectors to access foreign capital. Mainland-controlled firms accounted for 96 percent of these IPOs by number, more than double the percentage from 2018. Rather than suggesting that Hong Kong retains its role as a global financial center, this resilience marks its transformation into a key node in the CCP's technology ambitions and ties its financial and economic future to Beijing's priorities.

- Over the past year, the Hong Kong government has continued to systematically expand executive and security powers and give Beijing's security offices a greater role in local processes, eliminating the legal predictability and judicial independence that previously distinguished the city from the rest of China. The chief executive now has the unilateral ability to define what constitutes a national security matter and can apply the label retroactively to events that occurred prior to the passage of the National Security Law in 2020.

- Beijing's successful imposition of the mainland security regime in Hong Kong remains basically unchecked. Hong Kong authorities have jailed or quelled through repression elements of civil society that had resisted. The government may force anyone in Hong Kong to unlock personal devices and has restricted trade unions from engaging with foreign organizations. Many with the resources to do so have left Hong Kong. Voter participation has plummeted, reflecting widespread rejection of an electoral system that has forced out any elements disloyal to Beijing.

- The city's leadership has aligned its development goals more closely with the Mainland, even following the CCP in issuing Hong Kong's first-ever five-year plan. The government is diverting its resources toward supporting mainland ambitions for global expansion, technological dominance, and self-sufficiency even at the expense of its own fiscal health (see Figure 11). In turn, Hong Kong's business community incentives are aligned with China's agenda.

- Hong Kong's growing role in China's export-oriented economy and a resurgence in the financial sector led by Chinese tech stock IPOs have contributed to strong GDP growth. Beijing's cooptation of Hong Kong's economic system is more insidious in some cases. China is using Hong Kong to raise foreign capital for firms that face U.S. restrictions and/or serve the PLA.

- Hong Kong continues to enable China's support for autocratic regimes in Russia, Iran, and North Korea by acting as a central nexus for sanctions and export control evasion. The city's position as a global financial center and its lax regulatory environment for business registration combined with the leadership's refusal to proactively enforce sanctions have allowed corporations to complete billions of dollars of transactions that route dual-use components to Russia's war in Ukraine, facilitate Russia and Iran's crude oil sales, and allow North Korea to launder stolen cryptocurrency proceeds.

- Beijing's direct intervention in the city's economy has been limited to date, but the stage is set for major challenges ahead. Beijing has ratcheted up its own economic statecraft toolset with expanding export controls, limits on data and technology transfers, and tools to penalize companies complying with U.S. policies Beijing deems objectionable. ■

COMPREHENSIVE LIST OF **THE COMMISSION'S 2026 RECOMMENDATIONS**

The Commission considers 10 of its 30 recommendations to Congress to be of particular significance. These recommendations are denoted by an orange triangle ▲ next to the number.

Chapter 3: China's Other Front: India and the Future of U.S. Strategy in the Indo-Pacific

▲ **1.** The Federal Government has spent years building a wall against risky suppliers in strategic sectors. It now needs a purchasing strategy that makes trusted pharmaceutical production commercially viable. The central obstacle is commercial: manufacturers cannot justify investing in alternative sources of active pharmaceutical ingredients (APIs) and key starting materials (KSMs) without confidence that buyers will continue purchasing from them even when cheaper Chinese supply is available.

To break China's leverage over the supply of essential medicines, Congress should establish a Comprehensive Critical Drug Diversification (C2D2) program built around U.S.-India cooperation. The program should:

- Establish a pharmaceutical supply chain early warning mechanism for a list of essential medicines to identify APIs, KSMs, and critical intermediates and their production sites; identify single-country and single-facility dependencies; flag emerging disruptions; and direct purchasing and investment toward gaps.
- Authorize the U.S. Department of Health and Human Services to establish a Federal Trusted Demand Program, including multiyear commitments for essential medicines made with qualifying U.S. or trusted partner APIs and KSMs. The U.S. government should buy finished medicines it needs while making verified sourcing of critical inputs a condition for participation. The U.S. government should also ensure consistent purchase pricing across agencies. The program should:
  - Coordinate how participating agencies verify suppliers and the origins of their critical inputs, including subpoena authority to demand documentation;
  - Have the ability to make multi-year purchase commitments for essential medicines; and
  - Direct the U.S. government to work with providers to address cost disparities of buying medicines under long-term contracts.
- Include an initiative to support public and private investment in API and KSM production in India. For APIs, producers should be mandated to prove minimal and declining reliance on Chinese KSMs to receive the funding. The initiative should, to the maximum extent practicable, require matching funds from India and coordination with Indian producers to withstand predatory Chinese pricing.

▲ **2.** As the 14th Dalai Lama advances in age, China is preparing to turn his succession into an international contest over legitimacy and will likely use coercive tools to shape its outcome. India, which hosts the Dalai Lama and the Tibetan government-in-exile and shares a longstanding disputed border with China, is the center of gravity in this dispute.

Congress should make it the policy of the United States that the Gaden Phodrang Trust is the sole legitimate authority to identify and recognize the successor to the 14th Dalai Lama and that the United States will not recognize any successor selected or installed by the Government of the People's Republic of China. To carry out this policy and ensure U.S. government readiness for the Dalai Lama's succession, Congress should direct the Secretary of State to:

- Lead an internal interagency tabletop exercise on succession scenarios, with participation by the National Security Advisor, the Director of National Intelligence, and the Secretary of Defense, and brief the appropriate congressional committees on its findings within 180 days.
- Establish a senior-level channel with the Government of India for succession contingency planning, including intelligence sharing on Chinese influence operations, and report to the appropriate congressional committees on its status within 180 days.
- Conduct Track 1.5 and Track 2 dialogues and tabletop exercises with Indian counterparts on the political and security implications of succession scenarios.

- Coordinate with allies and partners on a diplomatic response that denies international legitimacy to any successor selected by the People's Republic of China.
- Counter succession-related influence operations by strengthening the Central Tibetan Administration's cybersecurity and resilience against China's cyber and artificial intelligence (AI)-enabled disinformation campaigns.

Congress should provide authorizations and appropriations to carry out these activities.

3. China's efforts to constrain India's regional influence and expand its military presence in the Indian Ocean underscore the importance of a stronger U.S.-India strategic partnership. The United States should deepen operational defense cooperation and foster lasting relationships among the next generation of American and Indian leaders.

Congress should:

- Direct the Secretary of Defense and Chairman of the Joint Chiefs of Staff to engage with their Government of India counterparts to strengthen coordination on undersea and maritime domain awareness in the Indian Ocean.
  - These efforts should prioritize moving beyond military exercises toward sustained operational cooperation, including systematic intelligence and surveillance information sharing, coordinated monitoring of Chinese naval and submarine activity, and improved procedures for responding to maritime threats.
- Create an Indo-American Strategic Leadership Exchange Program to forge generational ties among rising leaders in defense, government, business, and academia.

Chapter 4: China's Predatory Diplomacy in Latin America: Broken Promises, Harmful Practices

4. To enhance the capacity of Latin American countries to screen investments for economic and national security risks, Congress should:

- Direct the Secretary of the Treasury, in coordination with other members of the Committee on Foreign Investment in the United States (CFIUS), to establish a Foreign Investment Rapid Screening Team (FIRST) that trains and embeds in partner governments in Latin America. FIRST assistance should include:
  - Sending delegations to Latin America to develop screening mechanisms for investment and infrastructure projects as well as to train and work alongside procurement officers, auditors, and investment authorities on anticorruption, contract law, and corporate control structures;
  - Extending technical assistance to subnational governments, which often negotiate major investment and infrastructure projects but have limited capacity to assess national security implications;
  - Coordinating with the U.S. International Development Finance Corporation, Export-Import Bank of the United States, Millennium Challenge Corporation, and U.S. Trade and Development Agency to employ investment and technical assistance resources to incentivize partner countries in Latin America to develop investment screening mechanisms and mobilize U.S. and trusted capital as alternatives to untrusted investors;
  - Coordinating with the Secretary of State and organizations such as the National Endowment for Democracy to utilize their core institutes to strengthen the capacity of government and non-governmental organizations to support investment screening and related good governance initiatives.
- Appropriate funds for the U.S. Department of Commerce's Commercial Law Development Program (CLDP) to develop model legislation and regulations for strategic investment and infrastructure reviews.

5. The Chinese government has steadily expanded its influence in the multilateral development banks (MDBs), raising its shareholding and voting power, increasing its contributions, and positioning itself to shape lending priorities and institutional governance. The United States has not used its position as a top shareholder, including its unique veto power over certain governance decisions at the World Bank, to effectively advance U.S. interests and hold these institutions accountable. In particular, the United States has a strong interest in ensuring that MDB funds do not disproportionately benefit Chinese firms, yet there is no comprehensive, regularly updated strategy or public accounting of procurement awards to Chinese and U.S. firms across all the MDBs.

To focus engagement with international organizations—including international financial institutions (IFIs) and other multilateral institutions—on U.S. strategic interests and ensure adequate U.S. voice and representation at IFIs, Congress should:

- Direct the Secretary of the Treasury, as Chair of the National Advisory Council on International Monetary and Financial Policies, to:
  - Submit to Congress a strategy within 180 days to leverage the U.S. voice and vote at the MDBs—

the World Bank Group, the Inter-American Development Bank (IDB) and IDB Invest, the Asian Development Bank, the African Development Bank, and the European Bank for Reconstruction and Development—to counter China's action at IFIs and other multilateral institutions and to advance U.S. and democratic economic priorities, including responding to foreign adversaries' exploitation of IFIs. The strategy shall address, at a minimum:

- The development of programs to expand participation by U.S. and allied suppliers, and U.S. technology alternatives to Chinese options, in MDB-financed projects and procurements, coordinated with existing commercial advocacy mechanisms, including the U.S. and Foreign Commercial Service and the Advocacy Center;
- Supplier eligibility criteria grounded in security and technology provenance, together with an assessment of whether such criteria are required under each institution's existing procurement policy or would require action by its Board;
- A plan to counter exploitation of these institutions by China and other foreign adversaries, addressed by category, including continued borrowing by countries eligible for graduation, concentration of procurement awards, bilateral co-financing vehicles, secondment and staffing, and incorporation of China's technical standards into project specifications; and
- Measures to ensure transparency around beneficial ownership information for suppliers awarded financed contracts.

▷ Meet at least once a quarter with the Secretaries of State and Commerce to discuss U.S. priorities for IFI engagement.

▶ Amend the annual report required by Section 1701 of the International Financial Institutions Act on International Monetary and Financial Policies (22 U.S.C. §262r) to require for each MDB disclosure of: (a) the value and number of contracts awarded to suppliers registered in the People's Republic of China (PRC) and to suppliers identified as controlled subsidiaries of PRC-domiciled parents, with Hong Kong and Macau reported separately; (b) contracts awarded under section (a) reported as a share of internationally completed procurement and disaggregated by sector and borrower country; and (c) a description of actions taken to heighten scrutiny of state-owned enterprise participation in MDB-financed procurement.

▶ Restrict travel funding for relevant offices to non-essential expenditures, for example, limiting premium-class travel, reception and event expenses, large delegations, conferences, and new discretionary initiatives, until the Administration nominates senior director positions.

6. Congress should authorize and appropriate dedicated funding, through the Secretary of State, Secretary of Homeland Security, or Secretary of Commerce, to expand the "Rip and Replace" initiative beyond domestic networks to key strategic partner nations and key regions of strategic competition, beginning with Latin America and the Indo-Pacific. The initiative should utilize novel methods and technology from across frontier labs to identify, expose, and harden against weaknesses in Chinese-origin technology and software. It should work with nations to modernize equipment either by replacing certain critical assets within network infrastructure or software to ensure trusted standards are established. Specifically, the initiative should include the following provisions:

▶ Replace covered equipment. Building on the $8 million Panama pilot, fund the replacement of non-trusted telecommunications equipment in host nation infrastructure. Assistance should be conditioned on:

- ▷ Host nation operational control of replacement systems and host government concurrence in public announcements;
- ▷ A commitment not to reintroduce non-trusted equipment into assisted networks; and
- ▷ Sustainment included in each project.

▶ Assess, harden, and monitor software at scale. Direct the Secretaries of State and Homeland Security, drawing on the Defense Advanced Research Projects Agency (DARPA) and National Security Agency (NSA), to apply artificial intelligence (AI)-enabled vulnerability discovery and patching to:

- ▷ Triage host nation exposure through analysis of Chinese-origin firmware and software, producing a prioritized queue;
- ▷ Identify and remediate vulnerabilities in the software on which replacement networks run, including AI-assisted rewriting of legacy code into memory-safe languages where source code is available; and
- ▷ Provide interim detection and monitoring of covered equipment awaiting replacement. Analysis of equipment originating in China should inform prioritization and monitoring.

Congress should authorize and appropriate the multiyear initiative to execute country-level projects and require annual reporting to the committees of jurisdiction on sites remediated, conditions enforced, partner cost-share, and any reintroduction of covered equipment.

7. Congress should make it U.S. policy that China's systematic use of Port State Control inspections and detentions of Panamanian-flagged vessels is economic coercion and authorize the President to take all necessary and appropriate economic actions to counter China and support the Government of Panama in this dispute, including leveraging existing sanctions authorities and initiating referrals to the International Maritime Organization to establish a record of China's weaponization of port access as a tool of geopolitical punishment.

Congress should further direct the Federal Maritime Commission, which has already flagged the surge in detentions, to investigate the pattern and report findings within 90 days.

8. Congress should provide authorization and the necessary resources to the Secretaries of State, the Treasury, Defense, and Commerce to provide technical assistance to parliaments in Latin America to help draft and pass legislation to increase transparency and cybersecurity related to critical infrastructure through reforms to oversight, information security, and public contracting.

To expose the cybersecurity risks, lack of investment, and other hazards in infrastructure facilities with Chinese technology and ownership, Congress should:

- Direct the Director of National Intelligence to produce an annual unclassified assessment of, and brief other nations on, Chinese infrastructure presence across ports, energy, telecommunications, space, and other critical infrastructure sectors in the Western Hemisphere, including:
  - The security and economic risks associated with Chinese ports and equipment in the United States and countries in Latin America, including cybersecurity vulnerabilities, all potential vectors of military use and access, potential for economic lock-in effects and upcharges, and lack of capital investment.
- Direct the Secretary of State, in coordination with the Secretary of Defense, Secretary of Homeland Security, and U.S. Department of Transportation's Maritime Administration, to provide technical assistance to conduct inspections and establish a regional baseline for identifying and remediating vulnerabilities linked to China at strategic maritime chokepoints.
  - Where possible, the Secretary should seek cooperation with host countries for security audits of Chinese equipment and presence, identify highest-risk facilities, and recommend actions to ameliorate risk.

9. Across Latin America and the Caribbean, Chinese-linked criminal networks—money launderers servicing the region's cartels, illicit resource-extraction operations, and other currency channels that move value outside the correspondent banking system—have converged with an expanding PRC law enforcement presence that complicates, rather than supports, partner-nation cooperation with the United States.

Congress should direct the President to establish and appoint an executive agent to identify, expose, and disrupt Chinese-linked illicit narcotics suppliers, money laundering organizations, cryptocurrency networks, resource extraction networks, and other criminal facilitators in Latin America and the Caribbean. The executive agent should address risks associated with Chinese police and law enforcement cooperation in the region and should focus on the following activities:

- Disrupting Chinese money laundering networks.
- Strengthening partner capacity.
- Addressing risks from Chinese police training and security cooperation in the region.
- Improving information sharing.

Chapter 5: Active Intercept: China's Efforts to Narrow U.S. Undersea Advantage

▲ **10.** The Submarine Cable Act of 1888 only allows the United States to prosecute damage to subsea cables that occurs within U.S. territorial waters (i.e., within 12 nautical miles of its coastline) or damage caused by U.S.-flagged vessels wherever they operate. Current law limits the United States' ability to address other intentional damage to subsea cables landing in the United States or owned by U.S. entities. The United States must also address its limited repair ship capacity, which has led regulators to allow foreign adversaries to maintain U.S. cables that connect to the United States from a third country. This means provisions that would expand a trusted repair fleet and would ensure reinsurance for cable repair surge capacity during a crisis.

To address adversarial attacks on critical U.S. telecommunications infrastructure in international waters, Congress should:

- Amend the Submarine Cable Act to expand jurisdiction to prosecute acts of intentional sabotage against any critical undersea infrastructure landing in the United States or having any ownership stakes from U.S. entities.
- Strengthen undersea cable repair capacity by:
  - Barring the use of foreign adversaries' repair ships on U.S. cables and directing regulators to take associated action;

▷ In a manner consistent with current law, establishing a Pacific Allied Cable Repair Fleet, under which the Secretary of Transportation may enter operating agreements with qualified cable vessels flagged in the United States, and, where necessary, Japan, South Korea, and Taiwan; and

▷ Directing the Secretary of Transportation to provide insurance or reinsurance against war risks for foreign vessels engaged in cable installation and repair, in coordination with allied countries when possible.

11. To combat the People's Republic of China's "Transparent Ocean" and undersea modernization efforts, Congress should:

▶ Direct the Secretary of Defense, in consultation with the Director of National Intelligence and other relevant departments and agencies, to submit to the congressional defense committees a report, in both unclassified and classified versions, on China's "Transparent Ocean" efforts and associated programs. The reports should assess China's progress toward developing a persistent undersea surveillance architecture enabled by data fusion that integrates sensors and autonomous systems across domains from the seabed to space.

To ensure the United States maintains its advantage over China in cutting-edge autonomous and semi-autonomous undersea systems, Congress should:

▶ Direct the Secretary of Defense to submit to the congressional defense committees a classified report and briefing on its acquisition and program strategy for autonomous/semi-autonomous undersea systems. The report should address U.S. Department of Defense (DOD) capacity to surge production of these systems and detail how these platforms support U.S. Indo-Pacific Command's strategy in a Taiwan contingency.

▶ Appropriate funds for DOD to conduct a competitive, multi-supplier uncrewed underwater vehicle (UUV) hull-manufacturing qualification pilot that expands the industrial base beyond established defense contractors.

▶ Appropriate funds to expand DOD and other U.S. government agencies' procurement of UUVs. These agencies could include those falling under the U.S. Department of Commerce, U.S. Department of Homeland Security, U.S. Department of the Interior, and U.S. Environmental Protection Agency.

12. To maintain U.S. advantage in undersea surveying and seabed mapping, Congress should authorize and appropriate additional funds to the U.S. Department of Commerce's National Oceanic and Atmospheric Administration (NOAA) to expand seabed surveys and mapping operations in the Pacific, with a focus on working with the governments of the Pacific Island countries to conduct surveys in their exclusive economic zones (EEZs).

▶ An agreement with a country under this initiative should condition cooperation on prohibiting Chinese research vessel exploratory activity, seabed mapping, and seabed mining in its waters to the maximum extent permitted.

Chapter 6: The Price of Everything: China's Bid to Reshape Global Commodities Markets

▲ **13.** For over two decades, China has quietly pursued the development of domestic commodities exchanges, and expanded its production and processing of core commodities, becoming a key market maker in many segments and sectors. China is actively working to exert greater influence over global commodities markets with the aim of advantaging its domestic manufacturers and insulating itself against U.S. sanctions. To this end, China is pursuing numerous policies to expand its leverage, growing its domestic commodity exchanges, and opening more "in China for China" commodities trading to foreign participants. In recent years, China established the China Mineral Resources Group and other state instruments to consolidate purchasing of key commodities and has begun leveraging its position as a major buyer in physical markets to compel producers to use its preferred benchmarks and, in some cases, transact in RMB. China is building parallel systems that, absent action, may, over time, reshape the global landscape.

Congress should direct the U.S. Commodity Futures Trading Commission (CFTC) to monitor Chinese engagement and influence in commodities exchanges and warehousing and provide an annual report to Congress on activity, strategic risks, and efforts to coerce market participants as well as signs of market manipulation. To support this activity, Congress should:

▶ Expand CFTC foreign market surveillance and provide the CFTC the direction and, as needed, authority to monitor trading activity on Chinese exchanges, including but not limited to the Dalian Commodity Exchange (DCE) and the Shanghai International Energy Exchange (INE), with particular attention to participant concentration, state-owned enterprise positioning, and coordination among state-owned buyers. Current CFTC jurisdictional limits leave this activity unmonitored, and the China Securities Regulatory Commission does not make these data public.

▶ Direct the CFTC to monitor the development of China's futures markets, in particular for semiconductor, battery,

renewable energy, and critical industrial materials. Data on commodity pricing are difficult to obtain, particularly in markets where benchmark usage and settlement terms are embedded in opaque, privately negotiated contracts and are not systematically reported. Thinly traded contracts are susceptible to a risk of biased market data, putting U.S. producers at a disadvantage.

- ▶ Require disclosure of U.S. financial institution exposure to Chinese exchanges and other non-CFTC-registered foreign exchanges, as appropriate. Dodd-Frank reporting captures most U.S. derivatives activity on domestic and CFTC-registered foreign exchanges; however, many Chinese exchanges, including the INE, fall outside this framework, and these exchanges have not sought CFTC registration as Foreign Boards of Trade, meaning U.S. firms can trade on them without that activity being systematically captured in CFTC reporting.

14. Congress should strengthen the U.S. Department of Agriculture's (USDA) agricultural market intelligence and early warning capacity by directing the Secretary of Agriculture to enhance USDA's capacity to monitor Chinese agricultural commodity markets, supply chain flows, and state reserve management—such as dedicated monitoring of the Dalian Commodity Exchange's price signals and South American logistical flows controlled by Chinese-affiliated entities—and by providing sufficient appropriations to do so.

Chapter 7: Collect, Steal, Buy, Fuse, Monetize: How China Is Turning Data into Assets and Ammunition

▲ **15.** Data are a strategic asset that can drive scientific discovery, economic growth, and national security, but their value depends on the ability to organize, protect, and use them effectively. The United States needs a coordinated framework that makes data more accessible for legitimate uses, gives Americans control over their personal data, and prevents exploitation by China and other adversaries. An American Data Initiative would advance these goals while providing Americans meaningful control over their personal data.

Congress should establish an American Data Initiative to put American data to work as a source of national power, while preserving decentralized ownership, giving Americans control over their own data, and keeping their data out of the hands of China and other adversaries. Congress should:

Organize Federal Data

- ▶ Make the Administrator of General Services the Federal Chief Data Officer, with binding standards authority over all agencies and every agency Chief Data Officer appointed by and reporting to the Administrator, after consultation with the agency head.
- ▶ Direct the Administrator to govern all federal data by sensitivity and value, including in aggregate, and to make Data.gov the catalog of all federal data, open by default, with registered access for non-public data.
- ▶ Direct the Administrator to establish sectoral data foundries that produce AI-ready datasets, beginning with biology and embodied AI.
- ▶ Require the Administrator's approval of agency data budgets and bar funding for noncompliant data systems.
- ▶ Apply the confidentiality protections of Title 13 to personal data shared through the Initiative and record every access to non-public federal data in a tamper-proof log.
- ▶ Give the Government Accountability Office continuous access to those logs and authority to review any access to personal data and require an annual report to Congress with agency scorecards and privacy and civil liberties compliance audited by the Government Accountability Office.

Put Data on the Balance Sheet

- ▶ Make it U.S. policy that data held by federal agencies and U.S. businesses are an asset recognized on the balance sheet.
- ▶ Direct the U.S. Securities and Exchange Commission to require the Financial Accounting Standards Board to set standards for recognizing data as an asset within two years.
- ▶ Direct the Federal Accounting Standards Advisory Board to set comparable standards for federal agencies.
- ▶ Direct the Public Company Accounting Oversight Board to set matching audit standards.
- ▶ Direct the federal banking regulators to exclude data assets from regulatory capital.
- ▶ Condition the Governmental Accounting Standards Board's federal funding on comparable standards for state and local governments.

Let Americans Decide Who Gets Their Data

- ▶ Codify the core prohibitions of the U.S. Department of Justice's Data Security Program, including its bars on giving China and other countries of concern and covered persons access to Americans' bulk sensitive personal data and government-related data and its limits on onward transfer, and leave compliance requirements to regulation.
- ▶ Direct the President to designate an appropriate Cabinet or agency official to establish a national opt-in program under

which data brokers may not sell, license, or share Americans' personal data unless the consumer has opted in through a single federal portal that brokers must check before any transfer.

- Extend the Protecting Americans' Data from Foreign Adversaries Act to require data brokers, under a common statutory definition that applies throughout the Initiative and includes resellers and other intermediaries, to register with the designated official, hold them liable for transfers made without consent, bar transfers to persons under the jurisdiction of China or another foreign adversary regardless of consent, and make these obligations follow the data through every resale.
- Require data brokers, within two years, to obtain consent for personal data they already hold or delete it.

Bring Data Sales Out of the Shadows

- Define the rights in data that companies, governments, and consenting individuals can buy, sell, and license.
- Direct the designated official to register and supervise data exchanges, require data brokers, within two years, to sell personal data only through registered exchanges, and require exchanges to verify data provenance and consumer consent, screen buyers for ties to China and other foreign adversaries, including beneficial ownership and intended use, keep auditable records of every transfer, bar unauthorized resale and improper data combination, bar onward transfers to third countries without equivalent controls, meet security standards, and bar participants under foreign-adversary jurisdiction.
- Direct the Secretary of Commerce to open U.S. data exchanges to participants from allied and partner countries whose governments adopt equivalent consent, provenance, and foreign-adversary screening rules and extend reciprocal access to U.S. participants.

16. In 2024, the Commission recommended that Congress codify the authority established under the "Securing the Information and Communications Technology and Services Supply Chain" Executive Order (ICTS). The Connected Vehicle Rule demonstrates that the ICTS framework can work but it lacks a statutory basis and congressional direction to regularly identify, assess and mitigate risks across high-risk technology sectors.

Congress should codify the U.S. Department of Commerce's Office of Information and Communications Technology and Services (OICTS) and its ICTS authorities, provide dedicated funding and personnel, and require the office, in coordination with relevant federal agencies, to:

- Regularly assess categories of foreign-adversary information and communications technologies and services that could expose sensitive U.S. data, enable remote access or control, or compromise U.S. critical infrastructure.
- Report findings and proposed mitigation measures to Congress and initiate rulemaking for sectors posing national security risks, or explain why regulatory action is unwarranted.

17. To prevent China from stealing American data and harming American companies, Congress should establish a systematic effort against the ecosystem that supplies and monetizes China's cyber intrusions using "hackers for hire" and commercial cyber actors, by taking the following actions:

- Direct the National Cyber Director, in coordination with the Director of the Cybersecurity and Infrastructure Agency, the Director of the Federal Bureau of Investigation, the Director of National Intelligence, and the Secretaries of State, Treasury, Commerce, and Defense, to publish annually a list of foreign persons that:
  - Knowingly supply data, intrusion software, and botnet services to China's state-sponsored cyber actors or "hackers for hire";
  - Acquire or commercialize data or intellectual property stolen through those operations; or
  - Act as subsidiaries, affiliates, partners, joint ventures, licensees, or significant subcontractors of covered entities.
- Require within the 180-day period after the publication of each annual list:
  - The Secretaries of Treasury and State to determine whether blocking, financial, or visa sanctions are warranted;
  - The Secretary of Defense to determine whether government-wide or defense-specific procurement exclusion is warranted; and
  - The Chair of the Federal Communications Commission, where communications equipment or services are involved, to determine whether Covered List inclusion is warranted based on a determination by an authorized federal entity.
- Establish a program that would allow designated U.S. private sector entities to conduct cyber operations against approved foreign entities.
- Require reporting to the relevant committees of Congress, on: whether sanctions were imposed or list placements made; any identified statutory or resource gaps; enforcement coordination with allies; beneficial ownership and affiliate information; and procurement exposure across federal agencies.

Chapter 8: Silicon to Sovereignty: China's Bid to Control the AI Stack from Wafer to Weights, Part One

▲ **18.** The growing proliferation and adoption of Chinese open-weight artificial intelligence (AI) models in the United States carries national security implications for sensitive data, cybersecurity, and dependence on Chinese technology. Uncertainty about how these models behave in sensitive applications, what vulnerabilities they may introduce, and whether safeguards can adequately mitigate those risks warrants greater federal scrutiny. Congress should require enforceable protections for sensitive applications before these models become embedded in critical systems and costly to replace.

Congress should require the Secretary of Commerce, through the Office of Information and Communications Technology and Services (OICTS), in coordination with the Center for Advancing Innovation and Standards for Super Intelligence (CAISSI) and relevant federal agencies, to:

- Restrict deployment in sensitive applications unless safeguards are demonstrated. Within 180 days, identify sensitive uses—including systems controlling critical infrastructure, performing national security functions, or processing bulk sensitive personal data—and prohibit new deployment of covered models in those uses absent a time-limited authorization based on independently evaluated safeguards. Authorizations should address the model, its deployment environment, and its access to data, networks, and tools.
- Require identification and mitigation of existing exposure. Direct federal agencies and covered operators in designated sensitive sectors to inventory existing deployments and implement enforceable mitigation or replacement plans within deadlines established by the Secretary.
- Establish continuing security obligations. Require independent security testing, reporting of significant security incidents, reassessment following material modifications, and verification of compliance. Direct the Secretary to restrict or prohibit the commercial provision or deployment of designated models where identified risks cannot be adequately mitigated.
- Reduce strategic dependence. Require providers serving designated sensitive applications to maintain documented capabilities to replace covered models and migrate affected systems and data to alternatives meeting federal security requirements.

Within 180 days, the Secretary should also complete a consolidated assessment, building on existing federal evaluations, the National Telecommunications and Information Administration's (NTIA) open-model assessment, and federal supply-chain restrictions. The assessment should distinguish risks inherent in model weights from those arising from hosting, software, updates, and system integration; identify gaps in testing and verification; and inform subsequent requirements without delaying initial implementation.

Congress should authorize and appropriate funding, information-gathering and enforcement authorities, and penalties for noncompliance. The legislation should provide narrowly tailored exceptions for security research and authorized national security activities and require annual reporting to Congress on deployment exposure, compliance, mitigation effectiveness, and remaining dependencies.

▲ **19.** Americans should know when the government services they receive and the commercial products they use rely on AI models developed by Chinese companies. Clear disclosure would help consumers, businesses, and investors assess potential risks to data security, privacy, service reliability, and national security.

Congress should make it U.S. policy that Americans know when governments and businesses rely on AI models developed by Chinese companies. Congress should:

- Require federal agencies, and any state or local government or other entity that receives federal funds or federal tax credits, to disclose any use of AI models developed by an entity headquartered in, or organized under the laws of China, or owned or controlled by such an entity, including models fine-tuned on or derived from them, wherever they are hosted. Disclosure should appear in clear language on their public-facing platforms and in their filings with the federal government.
- Require businesses that use such models in any part of a product or service offered in the United States to consumers or other businesses to disclose that use clearly on their websites and in product documentation and treat failure to disclose as an unfair or deceptive act or practice enforceable by the Federal Trade Commission.
- Require reporting companies, as part of quarterly and annual disclosure filings with the U.S. Securities and Exchange Commission, to disclose as a material business risk the extent of their use of such models.

▲ **20.** Sustaining U.S. leadership in AI requires reliable access to advanced chips and the manufacturing capacity needed to produce them. Exports to China should not come at the

expense of capacity needed to support U.S. AI development and deployment. Requiring auditable exporter certifications would help ensure that export decisions account for these constraints and protect U.S. access to critical capacity.

Congress should ensure that AI chip exports to China do not divert capacity from the U.S. market, including by amending the Export Control Reform Act of 2018 (ECRA) to condition exports, reexports, or in-country transfers of advanced AI chips to China on exporter certification that they will not divert advanced semiconductor manufacturing or AI capacity from the U.S. market. The legislation should:

- Cover upstream capacity, including advanced-node wafer fabrication, high-bandwidth memory, and advanced packaging —not finished-chip inventory alone;
- Require auditable capacity-allocation data submitted to the Bureau of Industry and Security, subject to ECRA recordkeeping and enforcement provisions, including criminal penalties for false certification;
- Require the Bureau of Industry and Security to report annually to the committees of jurisdiction on certifications, validation methods, and exports coinciding with unmet U.S. or allied demand for equivalent capacity; and
- Prohibit regulatory waivers or narrowing of the requirement without an affirmative national security determination transmitted to Congress for a 30-day review period.

Chapter 9: Taiwan: A Crucial Window for a Critical Partner

▲ **21.** The People's Republic of China's (PRC) aggressive actions to reshape the Western Pacific and force unification with Taiwan are intensifying. Yet much U.S. and allied contingency planning focuses on large-scale invasion scenarios rather than coercion below the threshold of war. The United States needs a coordinated playbook with allies and partners for responding to a range of coercive gray zone activities by the PRC in the Indo-Pacific, specifically concerning Taiwan.

Congress should:

- Direct the National Security Advisor to develop a common playbook with allies and partners calibrated to counter multi-domain day-to-day PRC coercion. Departments and agencies involved in executing the playbook should develop tiger teams to address U.S. actions and coalition/allied actions under each area of responsibility. That playbook should provide a unified framework for participating nations to:
  - Share situational awareness and arrange pre-coordinated responses;
  - Counter disinformation and lawfare;
  - Expand combined coast guard operations with Taiwan and regional partners, including through multilateral initiatives; and
  - Support resistance against economic coercion.
- Amend and extend the Taiwan Enhanced Resilience Act to establish a Taiwan Democratic Resilience Initiative led by the U.S. Department of State, implemented through the American Institute in Taiwan in coordination with the Office of the Director of National Intelligence and other appropriate departments and agencies.
  - The Initiative should strengthen U.S.-Taiwan cooperation to support the resiliency of Taiwan's civil society and counter PRC united front activities, election interference, and disinformation campaigns. It should also include information sharing with U.S. allies and partners.
- Direct the National Security Advisor to lead an interagency process to develop a whole of government strategy for deterring, preparing for, and responding to coercive actions by the PRC against Taiwan that are intended to rapidly or substantially alter the status quo, but that fall below the threshold of a large-scale invasion or armed conflict.
  - It should include an assessment of contingency scenarios and for each, provide an assessment of indicators and warnings, likely PRC objectives, decision points, escalation risks, potential effects on Taiwan's access to critical goods and services, and options for coordinated actions with allies and partners.

22. As China's military capabilities expand and the regional balance of power shifts, the risk of conflict in the Western Pacific is increasing. Despite growing defense cooperation among the United States and its allies and partners, the absence of a formal multilateral security framework limits their ability to deter aggression and mount a coordinated response to attempts to alter the regional order by force.

Congress should direct the Secretaries of Defense and State to initiate consultations with U.S. allies on establishing a formal multilateral framework for collective defense in the Western Pacific, building on the multilateral defense cooperation directed by Section 1254 of the fiscal year 2026 National Defense Authorization Act. Where Section 1254 directs operational integration, this framework would institutionalize the political commitment to collective action needed to deter Chinese military aggression and provide the foundation for a Western Pacific Security Pact. The Pact should:

- Build on existing regional defense mechanisms among states with established foundations for expanded multilateral defense cooperation, primarily the U.S.-Japan-Australia-Philippines Defense Cooperation Council, and be positioned to complement multilateral security frameworks such as the Quad and AUKUS. Provide a pathway for accession by other states that share the Pact's principles and possess the willingness and capacity to contribute materially to peace, security, and collective defense in the Western Pacific.
- Establish a common commitment to collective defense under which members recognize that any major threat to, or violent breach of, peace and stability in the Western Pacific—or any military attack upon the members of this framework—threatens their shared security and national interests and commit to coordinate a powerful collective response to deter or defeat aggression and restore regional peace and stability.
- Accelerate the legal and military reforms necessary for collective defense, including combined contingency planning and exercises, integrated command and control, expanded intelligence sharing, reciprocal access, and integrated logistics to enable members to operate effectively as a combined force in crisis or conflict.

23. Beijing is using travel bans and other punitive measures to deter and intimidate foreign lawmakers from engaging with Taiwan, including barring four New Zealand legislators from the People's Republic of China in June 2026. By placing exchanges with Taiwan on the same footing as those with the UK, Canada, and Mexico, Congress would signal that parliamentary diplomacy with fellow democracies is routine, legitimate, and not subject to Beijing's veto.

The U.S. House of Representatives and Senate, respectively, should establish U.S.-Taiwan Inter-Parliamentary Exchanges, modeled on the established bilateral exchanges with the UK, Canada, and Mexico.

- Like those bodies, the exchanges would convene regular, structured meetings between members of the U.S. legislative branch and members of Taiwan's Legislative Yuan to discuss trade, security, technology, and shared democratic governance.

24. Taiwan is rapidly scaling its civilian and defense drone industries, building asymmetric capability that will be critical to prevailing in a potential future conflict with the People's Republic of China. Recent U.S. actions to broadly prohibit foreign drone imports stand to restrict a key market for Taiwan's drone makers and limit mutually beneficial collaboration with U.S. manufacturers.

Recognizing the benefit to U.S. national security of supporting drone industries of allies and partners at risk of conflict with adversarial countries, Congress should direct the Federal Communications Commission to limit its December 22, 2025 addition to the Covered List of uncrewed aircraft systems and their critical components, to systems and components produced by entities owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in 15 CFR §791.4.

Chapter 10: Hong Kong: Enabler of China's Global Finance and Technology Ambitions

25. Hong Kong's legal environment is deteriorating—not in a single dramatic event but through continuous, layered legislation that changes business risk year after year. Virtually any legal dispute involving a U.S. firm or its staff could be channeled into a national security case, and only a recurring statutory assessment keeps U.S. businesses informed.

Congress should require the Secretaries of State, the Treasury, and Commerce to jointly issue an annual Hong Kong Business Advisory informing U.S. firms of the legal, regulatory, financial, and reputational risks of operating in the Hong Kong Special Administrative Region. Each advisory would include the following:

- An assessment of developments over the preceding year, including new legislation, subsidiary regulations, enforcement actions, erosion of the rule of law, sanctions and/or export control evasion activities, and exit restriction risks.
- Updated guidance on risk exposure for personnel, data, intellectual property, and operations.

26. The U.S. Department of the Treasury has identified Hong Kong-based entities as key enablers of crypto-facilitated Iranian oil revenue laundering.

Congress should enact legislation to apply Primary Money Laundering Concern special measures, including correspondent account prohibitions, on Hong Kong Virtual Asset Service Providers that fail to prevent Iranian, Russian, or North Korean cryptocurrency trades.

Other Recommendations

The following recommendations build upon the Commission's work in recent years, including research, briefings, fact-finding trips, and conversations with key stakeholders.

▲ **27.** The Commission reaffirms its 2025 recommendation on post-quantum cryptography. Post-quantum risk is coming faster than the government is acting, and the federal response does not yet match the threat. China is investing heavily in quantum computing and has demonstrated sustained, large-scale collection against U.S. government networks. What Beijing steals encrypted today, it can read once a cryptographically relevant quantum computer exists. That same capability would also allow adversaries to forge the digital signatures that authenticate federal software, firmware, and certificates. The U.S. Government Accountability Office reports that agencies are only beginning migration, citing gaps in expertise, inventories, funding, and testing plans. At this pace, the government will miss its own 2030 target for critical systems. The government needs to treat this with far greater urgency.

Congress should:

- Require by statute that federal agencies migrate high-value assets, Federal Information Security Modernization Act (FISMA) high-impact systems, and public key infrastructure—including root certificate authorities and code- and firmware-signing systems—to National Institute of Standards and Technology (NIST)-approved post-quantum cryptography within 24 months of enactment. The statute should also set an accelerated, binding schedule for all remaining unclassified systems.
- Establish a dedicated post-quantum migration appropriation, separate from agency cybersecurity budgets, based on agency cost estimates certified by the Office of Management and Budget.
- Fund NIST's Cryptographic Module Validation Program and Cryptographic Algorithm Validation Program at levels sufficient to reduce validation wait times for post-quantum products.
- Require agency heads to certify progress to Congress every six months, with signed waivers for any missed milestone.
- Make crypto-agility and vendor post-quantum roadmaps conditions of federal information technology procurement.

28. People's Republic of China censorship demands on American companies are delivered privately and complied with quietly, leaving Congress, regulators, investors, and the public with no systematic picture of how widely Beijing's speech controls are being exported into the operations of U.S. firms. Mandatory disclosure corrects this information failure at minimal cost: it prohibits no transaction and forces no confrontation with Chinese law, yet it strips censorship demands of the secrecy they depend on, gives every firm legal cover to report rather than forcing each to choose transparency on their own, and equips U.S. policymakers with comprehensive data for trade and human-rights diplomacy.

Congress should:

- Require all U.S. firms operating in or doing business with the People's Republic of China to disclose to the Secretary of State and Secretary of Commerce and to each of the four congressional leaders every order, request, or directive received from Chinese government officials or their agents to censor, block, remove, or otherwise suppress free expression, including content directed at users outside China, within one month of each such request.
- Direct the Chair of the U.S. Securities and Exchange Commission to require reporting companies to disclose in annual and quarterly filings every order, request, or directive received from Chinese government officials or their agents to censor, block, remove, or otherwise suppress free expression, including content directed at users outside China.

29. As China expands its activities in space, the United States must be able to move at the speed of relevance to share intelligence with allies and partners in instances where such releases would strengthen collective action vis-à-vis China on space matters, while safeguarding sensitive sources and methods.

Congress should direct the Director of National Intelligence to work with the Secretary of State and other relevant executive branch agencies to create a process for accelerating the releasability of intelligence related to Chinese space activities to allied and partner nations that can favorably support U.S. competitive posture on space matters.

30. To expand defense technology cooperation and interoperability with trusted countries, Congress should:

- Make it U.S. policy to establish a standing partner track under AUKUS Pillar II.
- Direct the Secretary of State to propose the partner track to Australia and the UK.
- Condition partner track access on security benchmarks the Secretary of State certifies to Congress annually, including protection against access by persons under foreign adversary jurisdiction. ■

Physical copies of the full 2026 Annual Report to Congress are available upon request to congressional offices and other U.S. government entities.



2026 Report to Congress

of the

U.S.-China Economic and Security Review Commission

Executive Summary and Recommendations