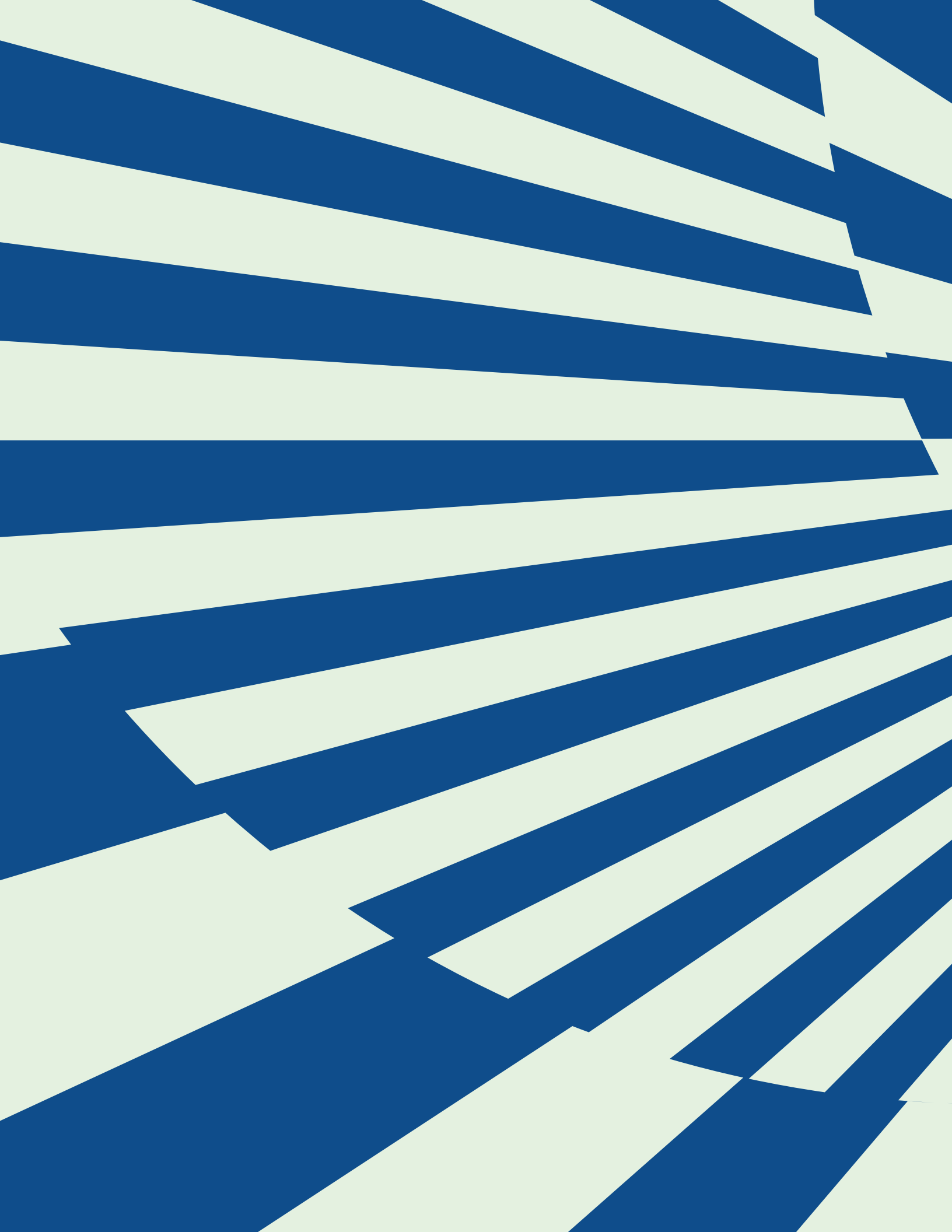




High Stakes: A Framework for Geopolitical Risk Management



U.S. Chamber of Commerce
Foundation



Contents

Executive Summary	8
I. Introduction	11
II. Firm Experiences: Survey and Interview Findings	17
III. Toward a Sustainable Decision-Making Framework to Address Geopolitical Risk	34
Annexes	46
Annex I: China Regulatory and Political Economy Landscape	48
Annex II: U.S. Legal and Regulatory Landscape	58
Annex III: National Security and Risk	68
Annex IV: Research Methodology	72

WE
BELIEVE
IN
BUSINESS

These words form the foundation of our credo and drive our mission to harness the awesome power of the private sector for America's good. As we begin this paper, these words take on special significance—guiding our effort to help businesses navigate an increasingly complex global economic order.

Since the Republic's earliest days, foreign commerce has been central to achieving unprecedented prosperity, not just for Americans but for billions worldwide. Our ability to deliver on the American dream stems from our unique entrepreneurial spirit, transforming ideas into goods and services that serve global needs. Through these trading relationships, the United States has built both economic might and diplomatic influence.

While we stand as an economic powerhouse, today's global marketplace is not without risk. Since World War II, foreign commerce has powered America's rise to unprecedented heights, carrying forward our founders' spirit of free enterprise. This model works—our economy is stronger than ever—but requires vigilance and adaptation.

Here at the U.S. Chamber of Commerce Foundation, we view global trade as the engine of opportunity. Yet in today's complex world, businesses from Main Street to Wall Street must prepare for the challenges of international competition. This report examines how leading companies manage these challenges in key markets, offering insights to help firms of all sizes make informed decisions from a position of knowledge.

This work represents an early step in our Global Threats Initiative, transforming pandemic lessons into durable solutions for future challenges. Forward-thinking executives understand that strategic planning creates opportunities throughout their ecosystem—benefiting employees, suppliers, customers, and communities alike. The pandemic demonstrated that when government and industry unite with common purpose, they unlock extraordinary capabilities to strengthen supply chains and drive innovation.

This report, developed in partnership with leading experts David Fagan and Meg Rithmire, converts insights into actionable guidance. Their expertise helps bridge the gap between academic understanding and practical business needs, offering a balanced framework for companies navigating complex international operations in an era of heightened security concerns.

Our approach acknowledges a fundamental truth: businesses need pragmatic solutions, not binary choices. By combining strategic foresight with practical risk management tools, we show how public-private collaboration can build lasting resilience that serves both business and national interests.

When firms successfully navigate geopolitical risks, the benefits extend far beyond their bottom line—they strengthen America's economic security and help ensure our nation's prosperous future.

Michael Carney

President
U.S. Chamber of Commerce Foundation

Author's Preface

This project started with a simple premise, a proposition, and an aspiration.

The premise was that businesses of all sizes were recognizing common challenges in rising geopolitical risks but much less common recognition—and understanding—of the tools to help manage that risk. For the majority, the intent was present; the path forward, less so.

That premise was borne from anecdotal experience, not systematic evidence, which led us to a proposition: We should test the premise through the collection of data and follow where that data would lead.

The aspiration was that, in doing this, the project could provide tools to help companies optimize decisions in the face of geopolitical risk—and that would ultimately, help reduce that risk incrementally which would benefit the companies and, since we were focusing on U.S. business, also benefit U.S. national security and economic resilience.

Put another way, we wanted to move past the common refrain “What is my competitor doing?”, and see if we could chart out tangible, actionable best practices that could be applied to, and embraced by, businesses of all sizes, in all sectors. This is our effort to provide a broader solution to risks that were related to commercial and national security.

The project, therefore, has been an exercise in optimism. At the same time, we have realistic expectations: We do not expect this to be a panacea, nor was that ever the intent. The framework that we set out focuses on process—and information—with a goal of making better, not perfect, decisions. And, while the focus is China—since, as the survey results indicate, that is overwhelmingly a focus for the business community—the framework in application truly is agnostic as to a country or an issue; it is a mechanism for repeatable, authoritative, well informed decisions, albeit, for purposes of this report, with a particular focus on China. The research that informs the report and recommendations was completed between June 2023 and September 2024, and the report itself was written before the end of the Biden administration. The second annex, on the U.S. regulatory

landscape, therefore includes only those measures implemented before January 21, 2025. Clearly, the global political landscape, including the relationship between the U.S. and China, continues to change rapidly, and we hope what follows will help U.S. firms build resilience during ever more turbulent times.

We benefited from the generosity of a great number of individuals and organizations as we did this work. For reasons of confidentiality, we cannot mention the names of the dozens of busy and well informed people from companies that spoke to us about their experiences and ideas—and more than 200 businesses that responded to the survey administered and gathered under the auspices of Harvard Business School—but we are grateful to each person who was willing to share their considerable expertise and their time.

We are especially indebted to the U.S. Chamber of Commerce Foundation for providing its sponsorship of the project and for its superb organizational effort and outreach. Michael Carney spearheaded this work; Pamela Wilson, Kelsey Margey, and Stephanie Johnson kept us afloat.

We also are grateful to the U.S. Chamber of Commerce for its support, and especially for the China Center. Jeremie Waterman, and Charles Freeman embraced the concept of this project at its earlier stage; the work reflected here literally would not have gotten off the ground without their support and their continued encouragement throughout the project.

For research help, we thank Dane Alivarius, Genevieve Hummer, Kate Swain-Smith, Brian Kim, and especially Dr. Bradley Holland. We were incredibly fortunate to work with the Association for Corporate Counsel, and we thank their research director Dr. Blake Garcia and President and CEO Veta Richardson.

A special thanks to Eric Rosenbach, who, in addition to serving on the Advisory Group, listened to us separately ponder this idea and had the foresight to connect us for this project. We also want to thank Covington & Burling LLP for allowing David Fagan to pursue this project and Harvard Business School for research and logistical support, especially Alain Bonacossa, Alma Castro, Tsedal Neely, and Rachel Talentino.

Last, an extraordinary group of business leaders, national security specialists, former policymakers, and academic specialists in law and economics served on an Advisory Group for the project from inception. Their guidance in structuring our inquiry and crafting recommendations that would be useful for firms and helpful for the public interest was immensely valuable. Their names are listed here, and we express our sincere gratitude for the time, connections, and deep insight they offered us.

Meg Rithmire

Co-Chair, Business Geopolitical Risk and Readiness Initiative Advisory Group
James E. Robison Professor
Business, Government, and the International Economy
Harvard Business School

David Fagan

Co-Chair, Business Geopolitical Risk and Readiness Initiative Advisory Group
Partner, Covington & Burling LLP*

**Mr. Fagan co-chaired this project in his individual capacity, and the work reflected herein is not that of Covington & Burling LLP or its clients.*

The Honorable Bruce Andrews

The Honorable Charlene Barshefsky, Parkside Global Advisors

The Honorable Karan Bhatia, Google

The Honorable Thomas Donilon, Blackrock Investment Institute

Kristen Eichensehr, Esq., University of Virginia School of Law

The Honorable Frank Jimenez, GE Healthcare

Christopher Johnson, China Strategies Group

Keith Kellison, Esq., UPS

The Honorable Ellen Lord, The Johns Hopkins University

Dr. Barry Naughton, University of California San Diego

The Honorable Eric Rosenbach, Harvard Kennedy School

The Honorable Pavneet Singh, The Brookings Institution

Executive Summary

Businesses face the most uncertain and complex geopolitical environment in memory. Although geopolitical challenges are not new to firms in the U.S. and beyond, the present moment is one of sweeping changes in domestic and international politics, rapid technological disruption, and expanded national security concerns amid truly global production processes, commercial competition, and capital investment practices. Russia's invasion of Ukraine; conflict in the Middle East; China's emergence as a global economic, technological, and military rival to the United States; climate change; the COVID-19 pandemic; the resurgence of industrial policy; and the growing use of national security-driven restrictions on global commerce (sanctions, export controls, investment screening, and more) have shaped, and may continue to transform, the contemporary global business landscape.

The expanding connection between national security concerns and global commerce is particularly acute, requiring businesses to consider deeply challenging scenarios—from the quick unraveling of global financial markets to ruptures in essential supply chains of energy, semiconductors, essential drugs, and food. The concerns of businesses cannot be limited to a narrow set of investments or trade in dual-use products covered by export controls; they must now cover a range of technologies, access to and transfers of data, development of power sources for computing, connectivity of devices, financial investments in sectors of competition, competition for raw materials, cyber and information security, and supply chain dependencies, among other considerations. Simply put, private firms, rather than governments alone, increasingly are viewed as on the front lines of national security, global power competition, and the stability of economies and societies.



This report was motivated by the desire to identify systematically how U.S. companies perceive and manage this geopolitical risk, to develop and articulate best practices in this environment, and, in turn, to distill and disseminate those best practices to business leaders and policymakers alike. In doing so, we seek to facilitate knowledge sharing and trust building between firms and the U.S. government and to provide recommendations for firms to build more robust practices of risk management for their own resilience and in the interest of the public good. That said, the report does not make policy recommendations, and we neither endorse nor criticize policymaking in our discussion. Our recommendations are directed at firms and intended to equip them to make better decisions on a sustainable basis no matter the policy direction.

Interviews with dozens of firms and two systematic surveys of firm representatives revealed that the People's Republic of China (PRC) is widely considered the primary geography of concern for firms of various sizes and in most sectors. Increasing geopolitical tensions between China and the U.S. and its allies, China's domestic turn toward security concerns over economic growth, and its enormous role in the global economy all present a unique set of challenges for firms. China's unique domestic political economy, which features a state that can mobilize large-scale resources and a powerful domestic legal regime, can provide the PRC government with considerable leverage over firms and market outcomes. That leverage, in turn, magnifies the concerns of the U.S. and other governments as they consider the implications of China's approach for their national and economic security.

This risk nexus is becoming more complex as the PRC pursues technological advancement, industrial upgrading, military-civil fusion, and self-reliance. Companies therefore face more commercial, operational, and reputational risks in their strategic planning related to China. Firms doing business in and with China—or with dependencies on supply from China or simply in competition with Chinese firms—have been exposed to these risks for some time.

But, as our research shows, the rise and global scale of Chinese competitors and China's global role make understanding China's political economic landscape—and U.S. reactions to China's practices—a growing concern even for companies not directly engaged in China.



In Section II, this report specifically presents the findings from interview and survey research. Further details on the unique features of China's environment relevant to business practices and risks, as well as U.S. regulatory and legislative actions that affect business practices in and with China, are included in the Annexes to this report. This additional detail provides context for the survey findings, which include the following results:

- Most businesses engaged in and with China do so in a multifaceted manner.
- Businesses perceive China as presenting considerable risk to company networks and data, intellectual property, and stable operations.
- At the same time, businesses perceive significant risks and costs to not being in China, including, among others, the need to be close to Chinese competitors and seek insights from the Chinese market and the scale and innovation power of China's production ecosystem.
- Firms are uneven in their development of due diligence, information collection, education, and risk monitoring practices to manage risks in China and beyond, with some applying sophisticated approaches but most applying a more ad hoc process.
- Nonetheless, firms generally are motivated to understand and adopt more resilient frameworks.

Given past and ongoing risk exposure in China, the inevitability of continued company engagement, and the difficulty of understanding and reacting to commercial and strategic threats presented by China's unique system, we recommend that firms develop a robust and resilient means of managing risk in and from China. Our recommendations specifically focus on the need for a decision-making framework, institutionalized in a "geopolitical risk management committee," to anticipate and manage China-related risk that is well informed, holistic, enduring, authoritative, and tailored.

A corporate governance framework, such as a geopolitical or China risk management committee with reporting to the CEO and ultimately the board, should have the following features:

- Receive information inputs on China's landscape and business exposure (**well informed**) from across the enterprise.
- Be staffed by representatives from applicable business units and operational functions (security and IT, legal, government relations, human resources, finance) and report to the board or at least senior management (**holistic and enduring**).
- Have the power to approve, amend, or recommend relevant business decisions (e.g., partnerships, investments, supply chain) with the ability to request more information or to decide on risk mitigation measures (**authoritative**).
- Be crafted in accord with the specific needs and structure of the firm and sectors of competition (**tailored**).

The goal of such a structured framework is to enable more informed decision-making by institutionalizing information collection, analysis, and decisional criteria; applying such tools in a manner tailored to the particular organization; and creating an articulable—and demonstrable—risk management process for both internal and external stakeholders.



I. Introduction

In the past decade, a series of acute crises signaled the end of a post-Cold War era of economic integration and has heralded a new one of geopolitical competition and insecurity. The result of these crises is an increasingly stressed geopolitical landscape and great economic competition to harness and control the development of new technologies, provide access to critical resources, and ensure national security in the context of economic interdependence. In this setting, businesses of all sizes and sectors must focus and plan for geopolitical risks and maneuvering in a polycrisis world in unprecedented ways.



Since 2018 alone:

- **The COVID-19 pandemic** shocked governments and companies as it exposed the complexity of the networked global economy. Cascading lockdowns, most notably the Shanghai Port Shutdown in the spring of 2022, had immediate and long-lasting consequences for global supply chains, and countries rushed to secure everything from critical health resources to basic household goods.
- **China dramatically accelerated its assumption of control over Hong Kong**, including through institutional restructuring and the adoption of the Hong Kong National Security Law, disrupting a major financial center, driving many businesses to relocate their Asia headquarters to other jurisdictions, and prompting the United States to respond by treating Hong Kong as legally equivalent to the mainland for trade controls and investment purposes.
- In February 2022, **Russia’s full-scale invasion of Ukraine**, accompanied by the announcement by presidents of Russia and China of a “no-limits friendship,” ended decades of peace in Europe and followed years of disruptive Russian cyberinterference in the media and electoral politics abroad. The United States, the European Union, and allies responded with unprecedentedly broad and coordinated sanctions on Russia—eventually including secondary sanctions on entities that have aided Russia—that immediately reconfigured the business activities of over 40,000 multinational firms with activities in Russia and, through second- and third-order effects on everything from insurance underwriting to commodities pricing, affected hundreds of thousands of firms outside Russia.¹ Three years later, Russia’s ongoing war against Ukraine continues to be sustained by unprecedented PRC support for Russia’s economy and defense industrial base, threatening escalation and geopolitical uncertainty.
- **Since August 2022**, China has demonstrated its commitment to press the bounds of its military, diplomatic, and economic response and to disrupt geopolitical relations and economic trade through the Indo-Pacific corridor, including coercive activity characterized by frequent incursions into air space and regular maritime exercises.
- **The Hamas attack on Israel** of October 7, 2023, unleashed broader conflict in the Middle East, including attacks on merchant ships in the Red Sea and risks of a broader war, resulting in additional global supply chain disruptions.

While the United States and other Western allies have had electoral shifts that impacted responses to these geopolitical developments, it is clear that within the business community (see Section II), the most significant risks for global companies are tethered to China’s emergence as a military, technological, and economic superpower and the U.S. response.

¹ https://www.rwellhausen.com/uploads/6/9/0/0/6900193/exitingrussia_wz_nov2024.pdf

The Challenge of China's Ascendance and Transformation

“For me, my agenda is number one: China, number two: China, number three: China... China issues are not just in China, but in every global market that matters to us, and my team's time reflects that.”

—Executive with risk management profile

Since China's opening to the world under Deng Xiaoping in 1978 and especially its accession to the World Trade Organization (WTO) in 2001, global firms have followed governmental policy encouraging market integration with China. China's large domestic market, skilled and motivated workforce, high rates of economic growth, and resulting innovation ecosystem have been extraordinarily attractive to global firms. By any measure, China is deeply embedded in the global economy. Unlike Russia, which primarily exports commodities, China is the largest trading partner for 120 countries, and third largest for the United States, with a complex basket of exports that indicates its centrality to global supply chains.

In recent years, however, governments and firms have had to contend with a transformed China under a resurgent party-state with a portfolio of activities, domestic and global, that have reshaped geopolitics and international markets. The severity of PRC's “dynamic zero COVID” policy took much of the world by surprise, with lockdowns continuing long beyond vaccination campaigns and normalization in the rest of the world. In early February 2022, before Russia's invasion, Xi Jinping and Vladimir Putin announced a “no-limits friendship,” and China has sustained support to Russia for intermediary goods that supply Russia's defense industrial base. The PRC's military build-up, focus on military civil fusion, and increasing gray zone and overt activities in the South China Sea have generated deep anxieties worldwide over China's ambitions and especially the potential for conflict over Taiwan.

Beyond these more recent events, the Chinese Communist Party (CCP), especially under Xi Jinping, has embraced a security focus in its interventions in the Chinese and global economy that has reconfigured strategic, commercial, and national security risks for firms and governments alike. Industrial targeting measures, most prominently the Made in China 2025 set of industrial policies focused on frontier sectors, have prioritized indigenous innovation with tremendous capital and political resources. Dramatic state investment and preferential policies in sectors like semiconductors, new energy vehicles, critical minerals, and more have completely reconfigured global competition in myriad ways. Blurred boundaries between the party-state and Chinese firms of all kinds, global acquisitions sprees, and massively scaled production have distorted global prices and challenged regimes of cross-border investment and trade with novel national security and competitive concerns.

Domestically, the CCP has sharpened its control over society through an emboldened surveillance state and repression. These actions have implications for global firms and supply chains, for example, with regard to the CCP's treatment of Uyghurs in the Xinjiang Autonomous Region. The U.S. government and other allies have placed sanctions on Chinese government officials and have enacted legislation—the Uyghur Forced Labor Protection Act—to preclude firms from doing business in or sourcing supplies from the region.

In mainland China, a suite of newly promulgated laws concerning intelligence, data security, cybersecurity, sanctions, and counterespionage, among others, has empowered state agencies to intervene in firm activities, further blurring boundaries between firms and the party-state and producing a nexus of risks for global firms. Companies engaged with or exposed to China must navigate Chinese and other countries' laws, which can conflict, and an organized and increasingly authoritarian Chinese government possesses significant leverage over firms that are embedded in China's economy in a multifaceted way.

When the PRC government targets advancement in specific sectors, especially those identified as critical to China's national security, the result can sometimes be coordinated efforts by many firms and government agencies to gain advantages in ways that present comprehensive risks for U.S. and global firms. In this way, the Chinese economic system fundamentally differs from one in which market forces and commercial logic alone drive firm decisions. In this environment, U.S. businesses must make commercial decisions with hard budget constraints and often with limited ability to track, anticipate, understand, or react to longer-term risks that emerge from China's strategic efforts.

The U.S. Response

“We are told to call the FBI if we suspect ‘insider threat’ problems or data collection from Chinese counterparts, but how are we to ensure that we don’t end up targeted by some politicians who want to seem tough on China and tough on corporate connections to China?”

—Compliance officer in large technology firm

Against the backdrop of intensifying competition with the PRC in military, economic, technological, and ideological domains, derisking or “selective decoupling” from China has taken firm hold in Washington as the operating consensus for both U.S. political parties. Successive administrations—the Trump and Biden administrations—have framed this dynamic as a long-term “strategic competition” with China.² National Security Advisor Jake Sullivan’s remarks in September 2022, in particular, capture a notable shift in tone in the U.S. government’s strategic thinking: “[W]e have to revisit the longstanding premise of maintaining ‘relative’ advantages over competitors in certain key

technologies...That is not the strategic environment we are in today...[w]e must maintain as large of a lead as possible.”³ The U.S. views China as “the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological capability to advance that objective.”⁴

The concern among Congress and the executive branch of the U.S. government is that existing regulatory and legal frameworks have not maintained pace with the changing geopolitical contours of U.S.-China competition, particularly in areas of advanced and emerging technologies, and are insufficient to address U.S. national security concerns. A **joint bulletin** from the Office of the Director of National Intelligence’s National Counterintelligence and Security Center is illustrative of this dynamic, warning that “U.S. emerging tech startups...face risks when seeking potential foreign investment” and that they should accordingly be wary of foreign investment “tactics” involving complex ownership, investments through intermediaries, and limited partner investments.

² Compare United States Strategic Approach to People's Republic of China, May 26, 2020, at p. 16 (“The United States recognizes the long-term strategic competition between our two systems. Through a whole-of-government approach and guided by a return to principled realism, as articulated by the NSS, the United States Government will continue to protect American interests and advance American influence.”), <https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.24v1.pdf>, and National Security Strategy, October 2022, at Introduction and p. 23 (“We are in the midst of a strategic competition to shape the future of the international order.”; “The PRC is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it.”), <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>. (Last accessible January 19, 2025)

³ Jake Sullivan, September 16, 2022, Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/>

⁴ <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>, p. 8. (Last accessible January 19, 2025).

As a result of this geopolitical dynamic to which the United States has been forced to respond, relations between the United States and China are framed as intensely competitive, where international partners and entities, as well as U.S. and multinational companies, are increasingly pressed to align with the U.S. response. As U.S. and allied governments struggle with a deepening set of challenges posed by China's rise, U.S. and multinational companies are at growing risk of reputational harm and regulatory restrictions regarding their commercial engagements with China, even when the specific behavior and engagement with China are not yet regulated by U.S. authorities.

In parallel, Congress has intensified scrutiny of business collaborations with China and has generated more aggressive legislative proposals to support a less permissive posture on China. In addition, U.S. lawmakers have pursued their investigative authorities to probe company practices and relationships in China. The House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (the China Select Committee) has launched investigations and issued letters to a range of major multinational companies, demanding disclosures of detailed information about existing and potential supplier relationships with Chinese entities.

As a result, U.S. business in China and with Chinese parties has come under unprecedented scrutiny, and the scope of business sectors seen as presenting national security risks has also expanded. Most importantly, the scope of U.S. government scrutiny and U.S. law is expanding to target previously unregulated relationships and processes, including internal corporate policies. For example, U.S. regulators, such as the Committee on Foreign Investment in the United States (CFIUS), will routinely explore both foreign investors' and U.S. parties' relationships in China as well as their internal policies and documents related to business in China. Meanwhile, the Department of Commerce has revised the Foreign Direct Product rule under 15 C.F.R. § 734.9, asserting the jurisdiction of U.S. export controls to cover certain items produced outside the United States.

In other words, a growing number of business relationships that are viewed as potentially advancing Chinese interests—even if in they were previously or are today in full compliance with U.S. law—have become more likely to create reputational and regulatory risks for U.S. and other multinational firms. As the scope of U.S. government scrutiny continues to expand, business relationships in China should be evaluated from the perspective of U.S. regulators and lawmakers who believe that previous and current laws are insufficient to address deepening geopolitical and socioeconomic tensions with China.





The Need for Geopolitical Planning, with a Particular Focus on China

Even with these risk dynamics, our research shows that many companies plan to continue engagement or expect to have continued exposure to China. There are multiple reasons for staying engaged. In broad strokes, the motivations are commercial and focus on the size and role of China in the global economy; the specific economic opportunities in the Chinese market; a desire not to be outpaced by competitors; a focus on accessing the best talent, wherever located in the world; obtaining insights that can be gained only by being in a particular market; and the challenges of exiting certain assets. Particular businesses, of course, weigh these factors differently, but our research clearly finds that, although economic growth in China has slowed and challenges to businesses are many, China retains a critical role in the global economy and is a continued area of focus for global firms. Put another way, China is by no means the only source of geopolitical risk, but it is the most salient for U.S. and global firms and therefore is the focus of this report.

As geopolitical competition intensifies and that competition is focused on economic dimensions, especially over shaping emerging sectors and national security concerns from interdependence, firms must broaden their competitive aperture to include geopolitical and national security risk in their decision-making in a structured way.

This report, commissioned by the U.S. Chamber of Commerce Foundation, aims to equip firms for resilience in such a context. The report is based on original research with U.S. and global firms, both interviews and surveys, the nature of which are explained in Section II. Our goal is to equip U.S. firms of all sizes and in all sectors with more information about geopolitical, political, and commercial risk entailed in doing global business in the context of China's transformation into a technologically advanced and global power and U.S. reactions to that development. To that end, Section III presents actionable recommendations for managing those risks through a corporate governance framework such as a geopolitical or China risk management committee.

Our report is intended neither to endorse nor to criticize policymaking, and we aim our recommendations at firms rather than governments. The goal is to inform and educate firms and the broader public about the risk landscape, points of vulnerability, and best practices with the ultimate aim of protecting prosperity and security and enhancing trust between policymakers and firms.

II. Firm Experiences: Survey and Interview Findings

Firms in the United States and beyond have faced a complex geopolitical environment overall, amplified by China's advancement of party-state goals and the U.S. regulatory responses outlined herein. In this section, we turn to data on how these firms perceive and manage these risks.

The data in this section come from three sources.

First, researchers from Harvard Business School (HBS) conducted interviews with personnel from more than 50 firms. Most of the firms were headquartered in the United States, but several were subsidiaries of parent companies abroad. Informed by this initial interview phase, the HBS researchers scoped a survey that was issued to two groups: (1) members of the Chamber of Commerce (USCC) and (2) chief legal officers of U.S. companies through partnership with the Association of Corporate Counsel (ACC), a nonprofit professional organization of legal officers in enterprises. Respondents from the ACC survey represented a broader array of U.S. firms of all sizes, including small and medium-sized enterprises as well as large multinational companies, whereas the Chamber survey was composed almost entirely of the latter group (large multinational companies).

Broadly, three main conclusions emerge from both the initial interviews and the surveys:

- China is the primary focus of perceived geopolitical risk among all groups, regardless of whether the company is engaged directly in or with China.
- Firms that are engaged in or with China do so in myriad ways and, therefore, encounter a complex web of risks.
- Firms have not been passive in the face of these risks but rather have tried to adapt company practices, often in creative ways. However, they have not always done so in a consistent or coherent fashion.

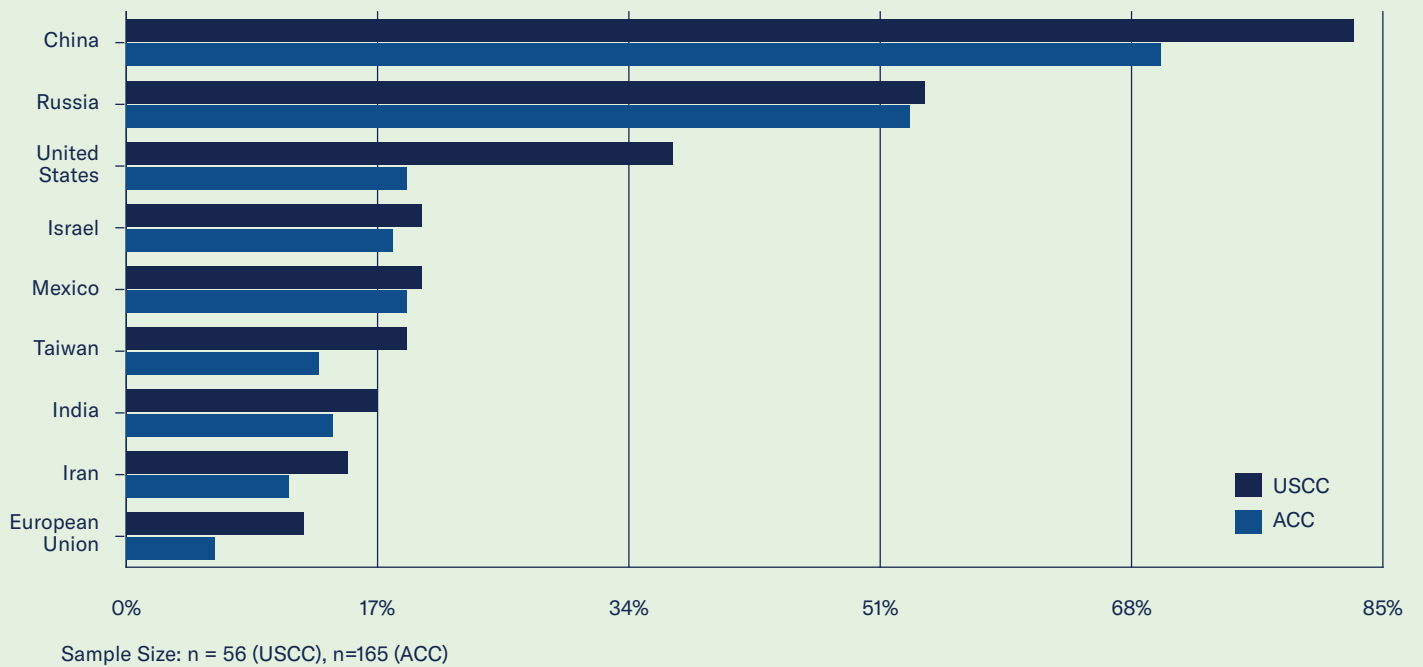
Many firm experiences, in turn, indicate opportunities to build more resilient and robust frameworks for managing risk. The final section of this report recommends such a framework.

China as a Primary Source of Perceived Risk

China emerged clearly as the primary source of perceived risk for all three populations. The survey asked respondents to identify their top three geographies of concern, and Figure 2.1 displays responses in percentage terms for both the Chamber and ACC populations. Eighty-three percent of USCC respondents cited China as a top-three geography of concern, and 70% of ACC respondents did.

Russia emerges as the second major site of concern, but, partly as a result of U.S. sanctions in the wake of Russia’s invasion of Ukraine in 2022 and partly because of the structure of Russia’s economy (considerably less interdependence with global markets than China), fewer companies report significant economic engagement with Russia. This makes the country more of an external source of threat for geopolitics and the global economy and less of an environment in which U.S. companies actively manage risks from engagements.

Figure 2.1: Survey Responses on Geographies of Concern



The U.S. was the third most prominent source of risk for USCC respondents, and a close fifth for ACC respondents. USCC respondents listed tariffs and import quotas, military or diplomatic crisis, political discourse affecting consumer behavior, export restrictions, local content requirements, and investment restrictions as the primary sources of concern with the U.S. On our reading, most of these factors are related to U.S. policy responses to PRC behavior that have reduced interdependence with China in targeted areas impacting U.S. national security and supply chain resilience. The focus of the report is on China, but we note that this focus includes the U.S.-China dynamics that have reshaped the business environment over the past several years.

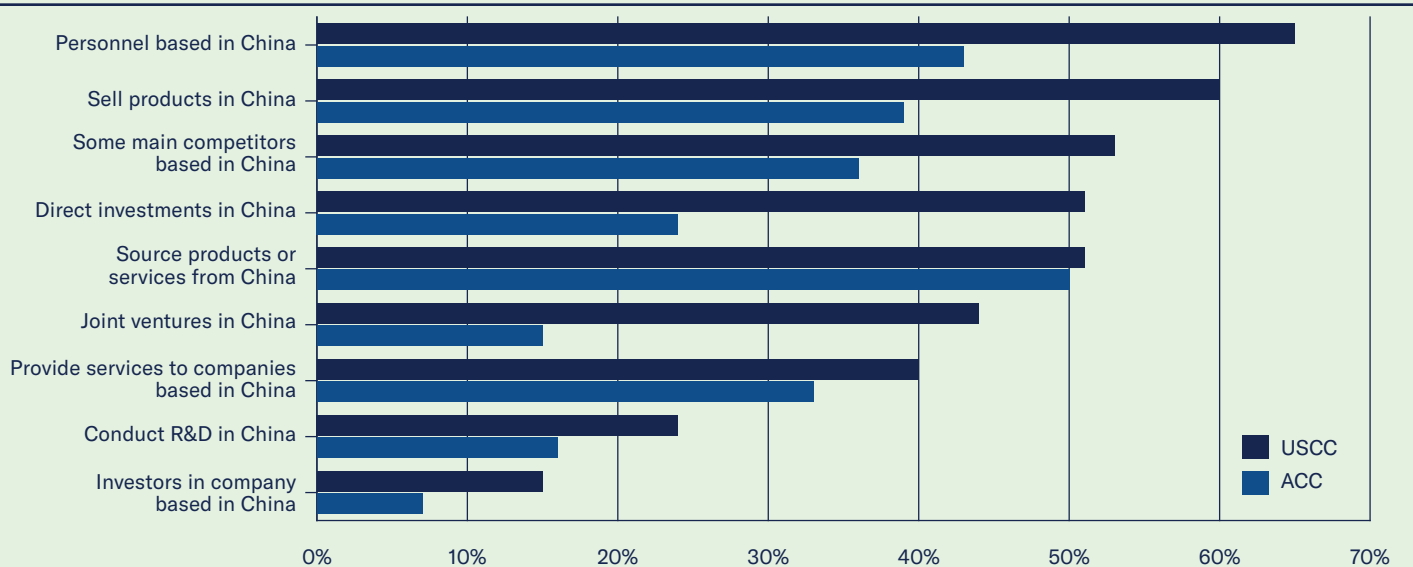
The survey results confirm that companies often have multifaceted means of engagement in and with China. Figure 2.2 shows survey results on how company representatives answered questions about their engagements in China, and Figures 2.3a and 2.3b visualize the multifaceted engagement of respondent firms.

For the USCC sample, 42.2% of companies that are engaged in China do so in all four types of activities, as defined on the next page, which is a strong plurality of those companies.

For the ACC sample, the largest group is composed of those that only buy or sell in China (24.2% of companies that are engaged), followed by companies that are engaged in all four types of activity (21.2%).

The multifaceted nature of engagements is expected as companies, especially large ones (such as those represented in the USCC sample), are attracted to China’s production capacity and potential as a market, but it also entails specialized risks. Multiple facets of engagement and modes of exposure can interact in ways that reduce comprehensive management of China risk for companies.

Figure 2.2: Survey Responses on Forms of Engagement



Sample Size: n=55 (USCC), n= 165 (ACC)



Figure 2.3a: Multifaceted Engagement: USCC respondents

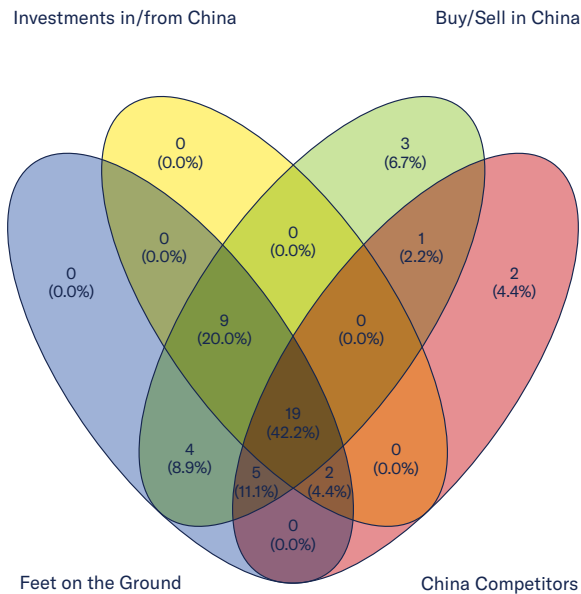
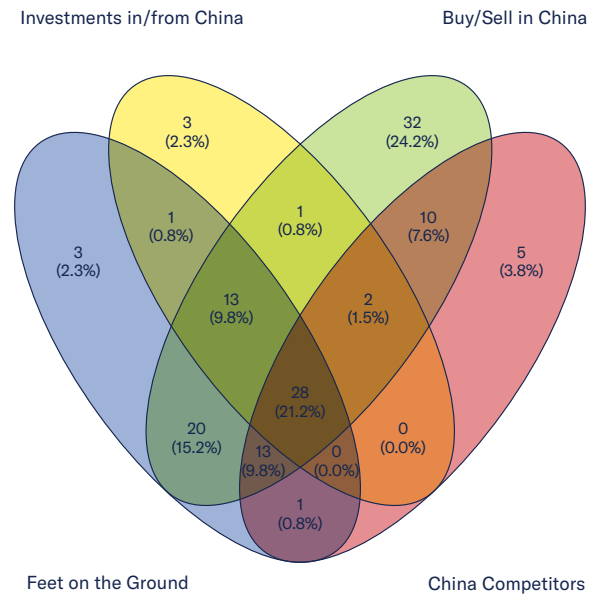


Figure 2.3b: Multifaceted Engagement: ACC respondents



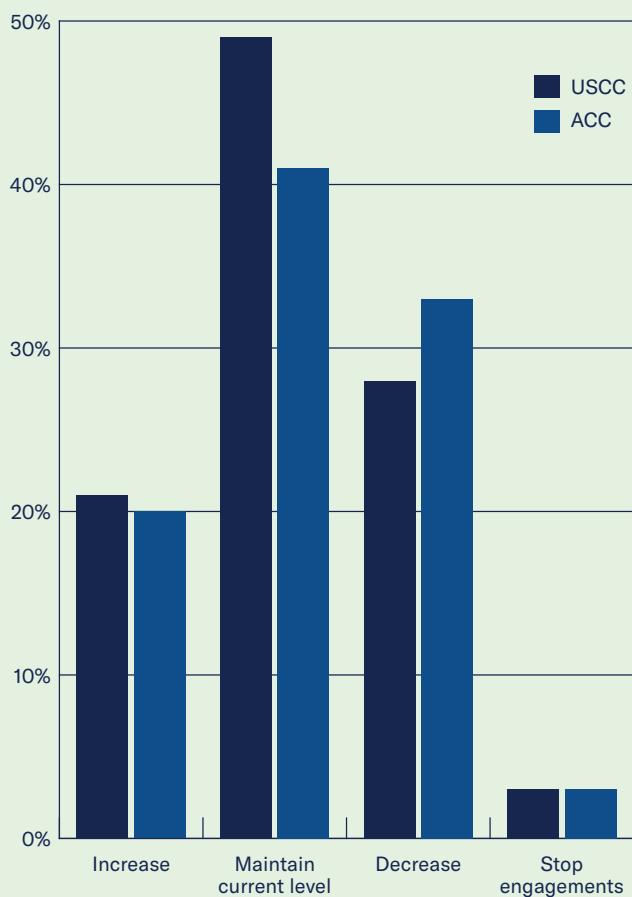
These figures plot overlaps in forms of engagement among firms engaged with China. The number in each segment represents the count of respondents in the USCC and ACC sample whose companies engage in all the types of engagement that overlap with that segment. The percentages reflect the percentage of companies in that segment relative to the total number of companies in the sample that engage with China.

- A company was coded as having **“feet on the ground”** if the respondent indicated that the company has personnel, joint ventures, or R&D in China.
- A company was coded as having **“investments in/from China”** if the respondent indicated that it has direct investments in China or that investors in the company are based in China.
- **“Buy/sell in China”** indicates that the company sources products or services to or from China.
- Companies with **“China competitors”** are those for which the respondent indicated that some of the company’s main competitors are based in China.

Many Firms Remain Engaged in and with China

Despite the fact that companies identified China as the primary site of geopolitical risk, many plan to remain in the market. Given the size of the Chinese market, the depth of China’s innovation ecosystem, and the significant scope of legacy engagements in China, most respondents in both the USCC and the ACC surveys indicated they plan to maintain or increase engagements in or with China (see Figure 2.4).

Figure 2.4: Survey Responses on Future Plans



Sample Size: Includes only respondents whose companies are currently engaged with China. n = 39 (USCC), n = 126 (ACC)

Firms across many sectors, including technology, agriculture, aviation, energy, and automotive, reported a variety of reasons that engagement or presence in the Chinese market remains imperative for competitive success as follows:

China Remains a Source of Revenue as Well as Innovation and Competitive Edge

- **Size of the market:** This rationale dominated in interviews and short-answer responses to survey questions, even given China’s macroeconomic problems. One consumer electronics company representative summarized: “Our sales growth is stalling in China with the economic slowdown, but it remains the largest middle class in the world. Even if they grow at 2% average over the next decade, that is a significant revenue source for us, and if we exit that market instead of managing it, we lose that market share to international and eventually Chinese competitors.” For many businesses, the earnings from China can help support their investment in other assets, including R&D, in the United States, contribute to returning earnings to their investments, and support other capital needs outside of China.
- Manufacturing firms have long benefited from the **co-location of R&D and production facilities** in China, the competitive pressures to lower costs for China’s middle market, and the scale potential of supply chains.⁵ One large manufacturer said of innovation dynamics there: “It is not labor costs at all [that keeps us manufacturing in China]; we are selling [products] to Brazilians and Indians that we never would have been pushed to make if we hadn’t been competing in China, with Chinese firms, for the Chinese domestic market.”

⁵ Jonas Nahm and Edward S. Steinfeld. 2014. “Scale-up Nation: China’s Specialization in Innovative Manufacturing.” *World Development* 54:288–300. doi: 10.1016/j.worlddev.2013.09.003; Brandt, Loren and Eric Thun. 2010. “The Fight for the Middle: Upgrading, Competition, and Industrial Development in China.” *World Development* 38(11):1555–74. doi: 10.1016/j.worlddev.2010.05.003.

- **Access to talent:** Companies that do R&D in China, and many companies that have China operations or have had some sort of R&D function in China (24% of USCC respondents; 16% of ACC respondents) value those functions because of the high level of skill of Chinese engineers and researchers and the relatively low cost. At least four companies reported assigning multiple China-based R&D teams to the same project to accelerate innovation at a low cost. That said, many companies report that the R&D they do in China is managed with an eye to intellectual property (IP) risk, for example, with employees there engaged only in “pure science” with no insight into application or “nonessential” to firm strategies and overall IP.
- **Critical knowledge of market dynamics from participation in China:** “Knowing the price of commodities is impossible if I am not in major agricultural markets in China,” to “Even though our JV has not been as successful as we hoped, we have no plans to exit because we need an ear to the ground in the Chinese market to know what our competitors are capable of,” to “Our worst fear is that we are unable, for political or regulatory reasons, to have any presence in China, and then are surprised when our competitors in China start challenging us globally with products we had no idea they were developing.”
- **Staying close to the competition:** Although company benefits of accessing China’s supply chain ecosystem are unsurprising, technology firms viewed supplying to Chinese tech firms and/or competing with them (many firms had both relationships simultaneously) as a necessary push to innovation: “Chinese IT firms are on the absolute frontier of innovation; we feel our interactions with them push us to meet them on that frontier, and so we worry about lost revenue, of course, but also lost opportunities at the forefront of what is next.” A technology company representative remarked that his firm plans to expand in China in both production and sales to the Chinese market: “Our strategy is not to protect IP. We know that as soon as we start making something in China, a competitor will make it faster and cheaper. That’s fine; actually, it just pushes us to stay at the bleeding edge of what the market wants and what it is possible to do.”

This is not to say that firms are ignoring China-related risk. Clearly, trends of diversification or exit from China are underway to varying degrees and can be challenging to quantify because of corporate reluctance to disclose such moves for fear of PRC roadblocks or retaliation. Although U.S. direct investment in China increased steadily between 2015 and 2020, U.S. foreign direct investment in China (FDI) has slowed, even plateaued, since 2021.⁶ Globally, foreign direct investment into China decreased by roughly 80% between 2022 and 2023. Many companies have diversified supply chains or otherwise sought paths to reduce their engagements in China for a variety of reasons.

⁶ The data from 2023 and 2024 are still being collated at the time of writing, but the U.S. Bureau of Economic Analysis shows that the U.S. direct investment position in China dropped slightly in 2020 and then increased only slightly in 2021–2023 (<https://www.bea.gov/sites/default/files/2024-07/dici0724.pdf>).

Some Firms Are Holding on to Some Investment Footprint in China in Anticipation of a Brighter Day

- **Waiting for resolution of China’s present structural imbalances:** Several firms in sectors such as manufacturing, technology, chemicals, and pharmaceuticals reported that overinvestment related to China’s industrial policy and investment-led efforts at economic recovery after COVID-19 have resulted in excess supply and lower margins in various product markets, or “overcapacity.” Many of these companies have internal projections indicating that supply and demand, and therefore prices, might stabilize in the next three to six years, depending on the sector. Those firms intend on holding their positions in China, even incurring losses, in anticipation of recovery and market rationalization.
- **Hope for a more reformist agenda:** Several interviewees, especially with deep expertise in their firms’ China business, noted that if the direction of policy becomes more reformist again, their shareholders would expect significant engagement with the Chinese market. These firms expressed concerns about missing out on a future upside with China, although they also acknowledged that there was a balance between such shareholder pressure and management and boards’ needs to evaluate national security and risk concerns.
- **Positioning on a sectoral basis:** One firm remarked that to exit China, even with JVs there suffering losses, would be “irrational”: “Our business has not been targeted in policies like Made in China 2025, but the moment [our sector] is mentioned in a five-year plan, things will take off quickly, and to miss out on that would be impossible from an innovation and sales perspective.” The company representative added that the firm would face “hard choices” about whether to bring their most advanced technology to China if the sector takes off: “We might lose the IP, or we might license and sell it, and lose it, but gain in the momentum before our Chinese competitors catch up.”

Yet Other Firms Are Remaining in China Because of the Difficulty of Exiting or Diversification

- **Stranded assets and challenges to divestment:** When regulations or informal pressures push companies to withdraw from engagements in China (e.g., unwinding a JV), they face many business and logistical hurdles. In particular, companies could not find buyers for assets in China, and many reported that Chinese buyers used the leverage of having a small universe of buyers to negotiate down prices significantly. Other companies reported in short answers in the surveys that they had multiyear commitments with suppliers and customers that limited their diversification or divestment choices.
- **Challenges to diversification:** In addition to this “stranded assets” problem, companies feared losing their ability to sell in Chinese markets and the costs to ramping up production outside China. In other words, even companies with a clear desire to diversify are often unable to do so. One scale manufacturer reports: “We can make [our product] with no Chinese components and no Chinese production, but it will take three years to realize, and costs will be 17% higher.” That company is executing that plan because its customers require supply chains without China exposure, but at least four other companies reported they had analyzed diversification and/or exit and concluded that the cost-benefit analysis did not leave them optimistic. One company responded in an explanation for plans to maintain engagements in China: “We cannot avoid China. Components and/or ingredients can be sourced cheaper. It has a massive population, which could become customers. If we are not active in the market, then someone else could take over our IP, and we wouldn’t know it.”

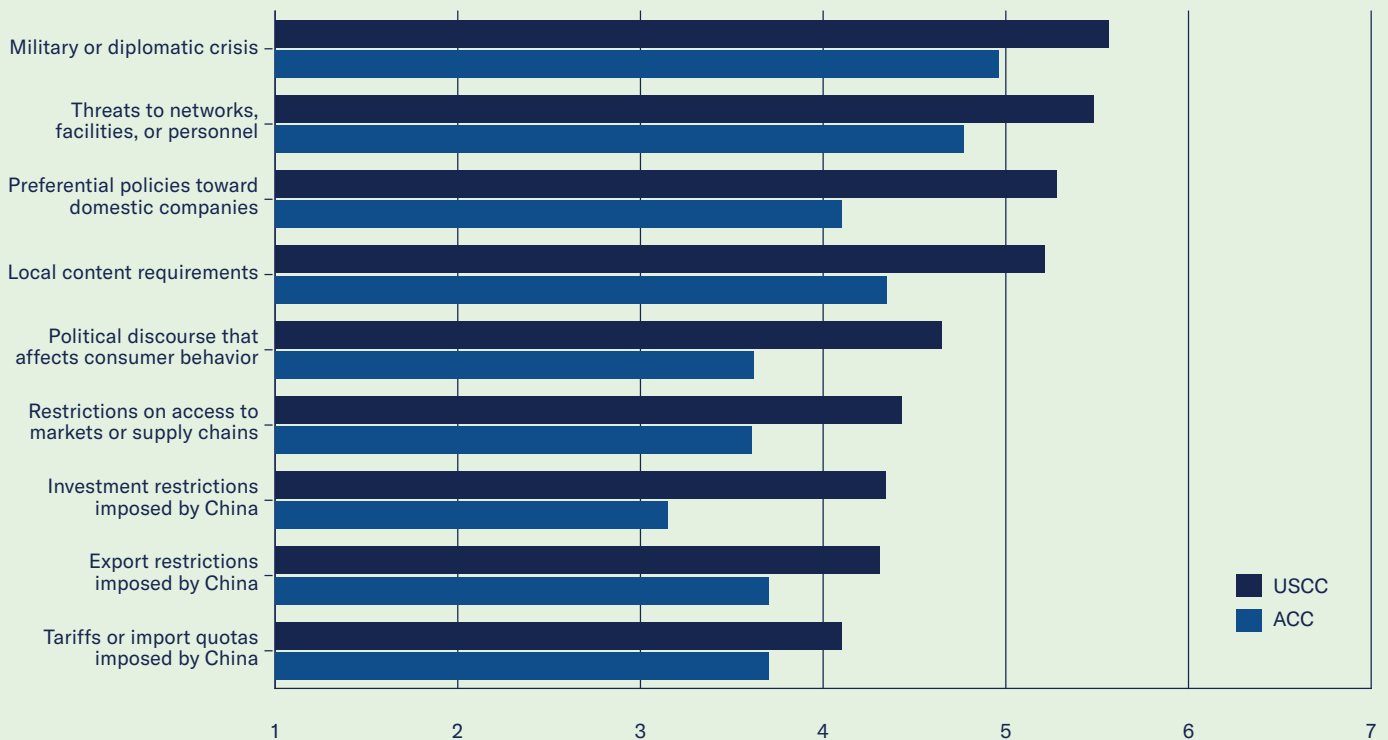
Sources of Concern

Although some firms are continuing to grow their investments and others are holding their positions, we asked in surveys and interviews about both increased sources of risk and how those risks are perceived to affect business activities. Survey responses are in Figure 2.5. In general, these risks fall into three areas and reflect the following:

- 1 Enhanced laws and regulations, as well as aggressive “enforcement,” justified on “security” grounds and effectively restricting access to China’s economy
- 2 Commercial and strategic threats from China’s emphasis on domestic innovation
- 3 Broad concerns over growing instability in cross-straits relations

Figure 2.5: Survey Responses on Exposure to Risk in China

Average response on 1-to-7 scale where 7 is “very concerned” about:



Sample Size: n= 48 (USCC), n=151 (ACC)



1. Securitization of China's Political Economy

The CCP's resurgent role in the Chinese economy is both a reaction to and further cause of China's economic slowdown.⁷ U.S. firms, and even Chinese firms, are troubled by a lack of high-quality data on the Chinese economy and barriers, legal and otherwise, to conducting due diligence and market research. Most companies expressed concerns over China's policy direction and the opacity of its economic conditions.

- **Legal environment:** Relatedly, the promulgation of national security and data and cybersecurity laws in China has produced a chilling effect on firm activities and has raised the costs of doing business in critical sectors. In interviews, at least six companies reported visits from the Chinese Ministry of State Security (MSS) to assess how they were dealing with data in the context of China's 2021 Data Security Law, and at least two companies expressed that these visits seemed designed to intimidate. More generally, laws like the Counter-Espionage Law (2023) seemed to alarm companies and individual executives, as the laws give broad legal authority for the MSS to investigate and potentially detain firm personnel. Importantly, the specific concerns were that local MSS branches were becoming emboldened to undertake more investigations, and the definition of national security-relevant knowledge seemed to include activities like due diligence and market research. Companies varied in their concerns about the laws, with some expressing extreme concern and others relatively dismissive of this tightening legal environment. Advisory services firms (legal, consulting, and so forth) expressed the greatest concern, especially given 2023 raids on Bain & Company in Shanghai and the Mintz Group in Beijing. Public information (i.e., not obtained in interview research) indicates that Chinese nationals were detained in both raids, and the Mintz Group was fined \$1.5 million for “unapproved statistical work” and “foreign-related statistical information.”⁸
- **State interventions with facilities and personnel:** Many firms competing in China expressed risk concerns in terms of personnel in China and noted upticks in site visits from Chinese security personnel, especially the MSS.⁹ Critically, most firms are not always certain about the frequency of these visits or the reasons behind them. However, discussions with U.S. security-related advisory service providers suggested that these visits are frequently coordinated and systematic. In addition to site visits, firms report that China-based personnel receive “invitations for tea” with local government and sometimes central government personnel. One company that supplies the U.S. federal government, including the Department of Defense (but does not manufacture products in China that are supplied to the U.S. government), reported persistent tea invitations and perceived pressure to both convey information about how the U.S. government protects information security and also to “choose supplying Chinese firms over supplying the U.S. government.” Most companies answered questions about tea invitations with expressions of concern that they are certain it happens but do not know when and why, and they do not have clear means of eliciting and acting on this information. Firms with connections, even indirect, to new outbound investment restrictions note an increase in tea invitations and MSS visits or rumors of such in their networks. One interviewee stated that Chinese government officials appear eager for information from firms on which sectors are likely next to face such restrictions.

⁷ Margaret M. Pearson, Meg Rithmire, and Kellee S. Tsai. 2022. “China's Party-State Capitalism and International Backlash: From Interdependence to Insecurity.” *International Security* 47(2):135–76. doi: 10.1162/isec_a_00447.

⁸ <https://www.reuters.com/world/china/china-fines-mintz-15-mln-unapproved-work-after-raiding-its-beijing-office-2023-08-22/>

⁹ <https://www.prcleader.org/post/piercing-the-veil-of-secrecy-the-surveillance-role-of-china-s-mss-and-mps>

- **Exit bans** have increased in the past several years. Although no systematic data exist for obvious reasons (media and government attention is not necessarily helpful for firms and individuals dealing with exit bans), scholars have documented at least 100 cases.¹⁰ These bans seem to typically target affiliates of firms with contract or judicial disputes in China and are frequently part of the CCP's disciplinary and anti-corruption efforts to prosecute criminal activity and recover fugitives (Operation Foxhunt and Operation Skynet).¹¹ Even with the release of some U.S. prisoners, a lowering of the U.S. Department of State's Travel Advisory, and the release of some U.S. citizens being detained through exit bans, the general opacity of the PRC judicial system nonetheless means that companies and their personnel in China will continue to face uncertainties, often not knowing if there is a dispute or if their firm is connected to a dispute between other parties. The PRC government has refused to renounce the practice of what one interviewee flagged as "commercial hostage taking," and exit bans can apply when firms offend the Chinese government or are engaged in activities the PRC designates security relevant, such as sensitive data collection or due diligence.

2. Commercial and Strategic Threats from Domestic Innovation Drive

- **Informal domestic supplier pressure:** U.S. companies that sell to Chinese firms have experienced drops in demand as their clients suggest they are pressured to turn to Chinese suppliers. Several explained efforts to cooperate with Chinese firms to help clients source domestically, and others stated that they had market exit strategies because their access to Chinese firms as clients has dramatically diminished. This was particularly the case with U.S. companies providing services to Chinese firms within China. Many of these same U.S. firms who are withdrawing under pressure from the domestic market see tremendous growth in their provision of services and products to Chinese companies outside of China, and they continue to provide services for multinational firms that do business inside China.
- **Formal domestic supplier pressure:** In addition to informal pressure via clients in China, U.S. firms are aware of formal regulations preferencing Chinese suppliers in specific sectors (especially technology).¹² The Chinese government increasingly prohibits technology and software produced outside China's borders to be used in government procurement in China. As a result, several firms are locating their entire production processes in China for the Chinese market, whereas others are strategizing for exit in anticipation of losing market access altogether. One company representative said plans for decreasing engagements with China come from "increasing geopolitical and economic tensions as well as competition from local providers/barriers to success for multinational entities." Another company suggested that "Western companies are at a competitive disadvantage that cannot be overcome" in competing in China's market.

¹⁰ Jack Wroldsdien and Chris Carr. "The Rise of Exit Bans and Commercial Hostage Taking in China." MIT Sloan Review. Vol. 65, Issue 1 (November 2023).

¹¹ "Operation Foxhunt" (2008–) was the predecessor to "Operation Skynet" (2014–), both focused on targeting "economic criminals" to recover Chinese assets and people from abroad. Chinese media and government reports conclude that, combined, these campaigns have resulted in the apprehension of more than 10,000 individuals and the recovery of more than 20 billion RMB in assets between 2008 and 2021. See Meg Rithmire. 2023. *Precarious Ties: Business and the State in Authoritarian Asia* (Oxford University Press): pp. 247–8. FBI Director Christopher Wray and others have expressed concern that these efforts to track and recover individuals and assets abroad constitute international expansion of the CCP's authority and "transnational repression" outside of China's jurisdiction. See <https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122>.

¹² <https://www.uschina.org/reports/government-procurement-and-sales-state-owned-enterprises-china>. <https://www.prnewswire.com/news-releases/futurelogic-releases-china-tech-decoupled-report-providing-insights-on-chinas-xinchuang-industry-301433437.html>

3. Deteriorating Cross-Straits Relations

The relationship among the United States, China, and Taiwan figures prominently in medium- and long-term thinking of nearly every U.S. company. Many firms have engaged experts and consultants to consider what scenarios might materialize in the China–Taiwan relationship, including “tabletop” exercises through which companies explore how various scenarios affect their businesses. Almost universally, large companies expressed concern that they “cannot prepare adequately for these scenarios.” As one interviewee put it: “There is no way to hedge or prepare for an invasion or a blockade. You can do an exercise to see how it affects you, but the result is always catastrophic, and it is a bottled water situation.” These sentiments from interviews mirror research showing the potential effects on the global economy from a crisis in the Taiwan Strait. The scenarios are contingent on China’s actions, the U.S. response, and China’s further responses, but it is clear that global industries from semiconductors, financial markets, and global shipping would experience crippling disruption and affect countries and sectors globally.¹³

Concerns about Taiwan and the U.S.-policy response to a Taiwan contingency (especially sanctions and Chinese responses) were the main motivations for decreasing engagement with China or diversification. Noticeably, companies see the supply chain risks as dyadic, with pressure from concerns about China and concerns about U.S. restrictions. In interviews, we learned that companies see hedging these risks as expensive and difficult, and although many firms that are decreasing engagement or diversifying cite supply chain risks, most plan to diversify rather than exit China entirely. Many companies also caveated responses in terms of what they “aim” or “intend” to do rather than descriptions of actions they have already taken.

¹³ <https://www.atlanticcouncil.org/news/press-releases/atlantic-councils-geo-economics-center-and-rhodium-group-release-major-report-on-sanctioning-china-in-a-taiwan-crisis/>; <https://www.atlanticcouncil.org/in-depth-research-reports/report/avoiding-entanglement-g20-responses-in-a-taiwan-crisis/>

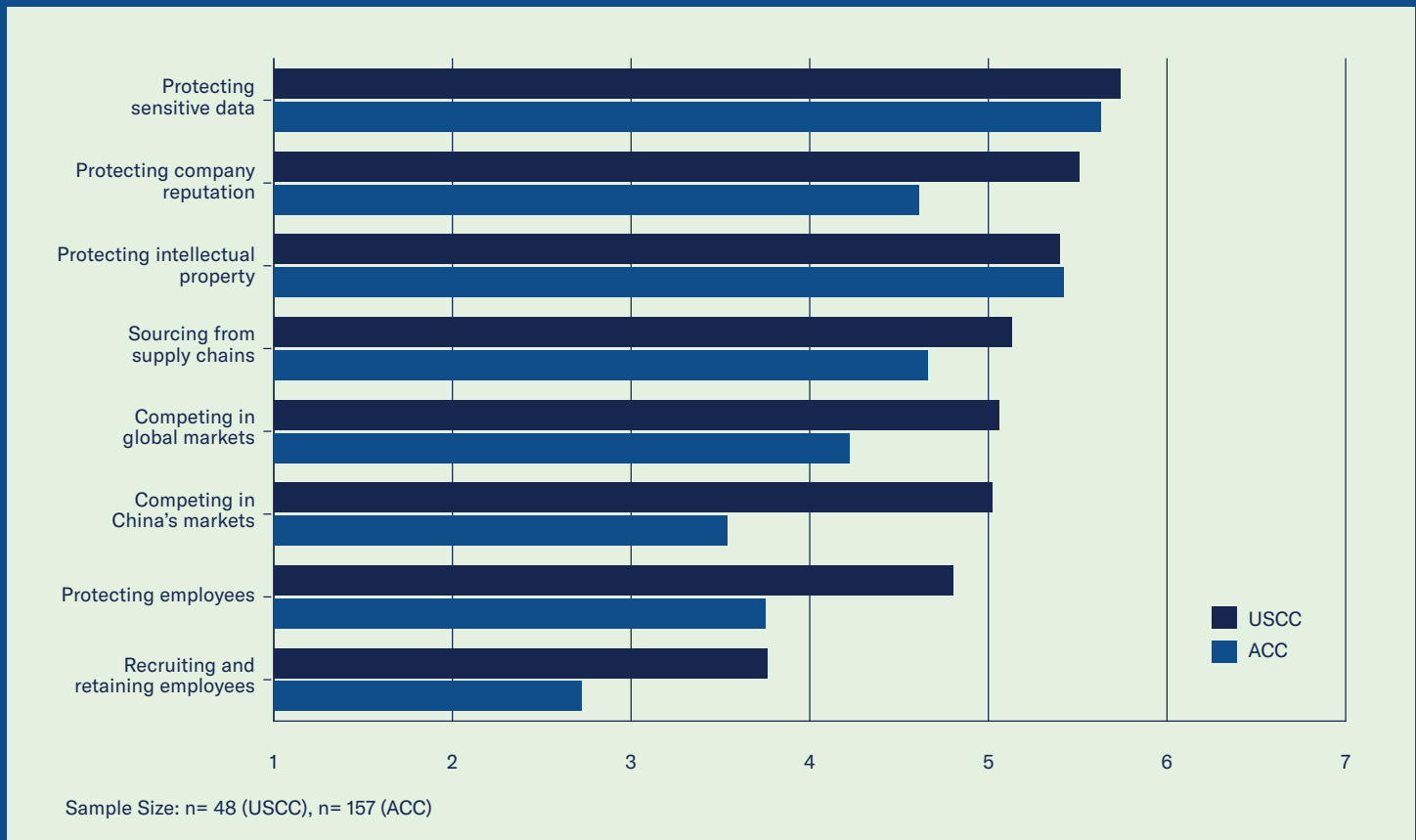


How Business Are Responding to Geopolitical Concerns and Realities

The U.S.-China relationship and the Chinese business environment have material impacts on companies, whether they engage deeply in or with China or not. Figure 2.6 shows how respondents perceived risk to different parts of their businesses.

Figure 2.6: Survey Responses on Effects of Risk

Average response on 1-to-7 scale where 7 is “very concerned” about:



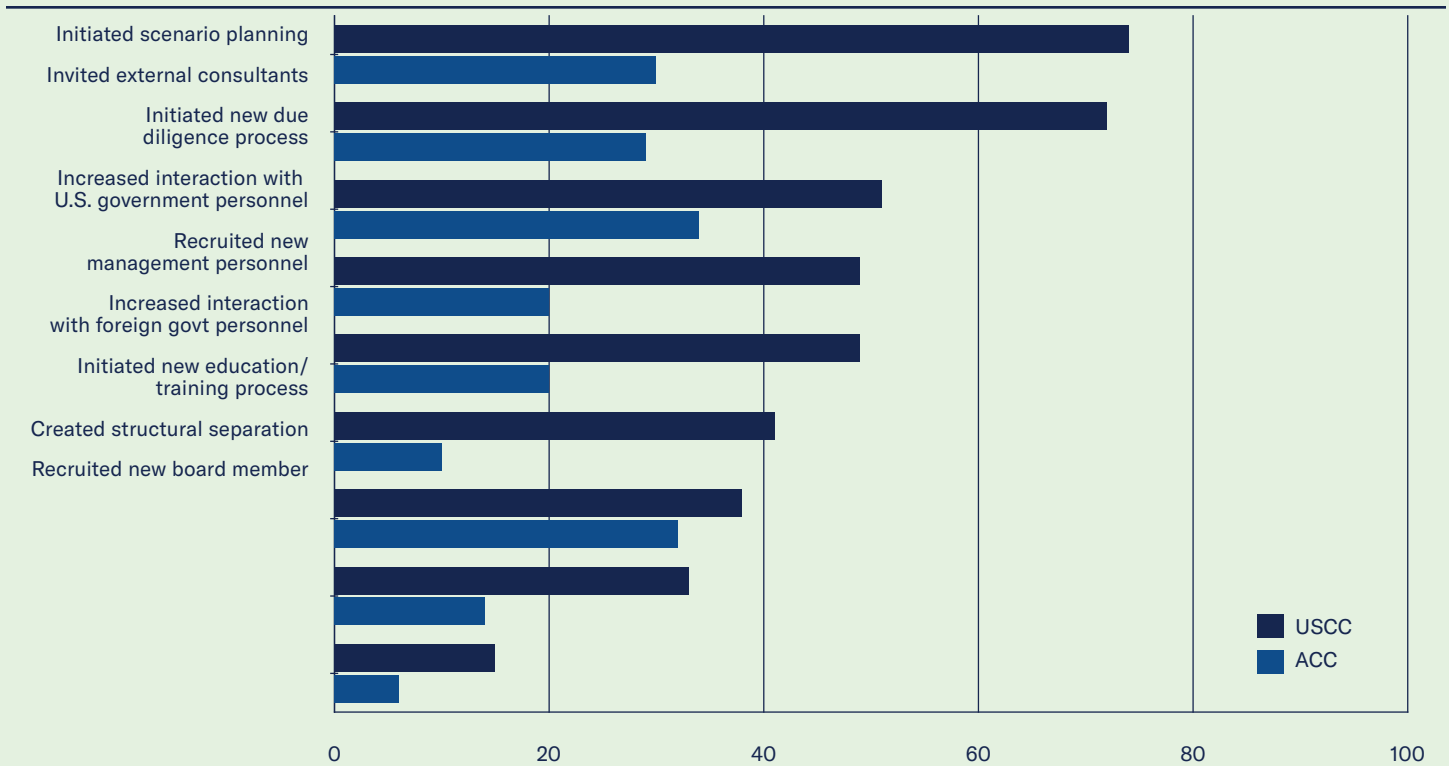
Firms are responding broadly in six ways:

- 1 They are devoting more firm resources to mitigating perceived risks.
- 2 They are placing more emphasis on strategic planning.
- 3 They are overhauling their decision-making processes when it comes to China-related transactions.
- 4 They are overhauling their information collection and dissemination strategies firm wide to better address risk in China.
- 5 They are upgrading their engagement in Washington on China-motivated legislation and regulation that are likely to affect their businesses.
- 6 They are beefing up their compliance operations to account for increased regulations and the associated risks of running afoul of proliferating laws and rules that mandate accountability and transparency and increasingly circumscribe commercial opportunities.

More Firm Resources for Managing Risk

Overall, survey data confirm that firms are devoting increased resources to address China-related risk in targeted ways. Figure 2.7 shows responses to geopolitical risk (generally, not just China focused) from both the USCC and ACC respondents. Clearly, well-resourced and larger firms, typically the USCC respondents, have devoted more resources across a spectrum of activities, with over half reporting new due diligence processes (51%) and one-third (33%) reporting “structural separation” within the organization.

Figure 2.7: Survey Responses: Firm Actions on Geopolitical Risk



Sample Size: n= 39 (USCC), n = 208 (ACC)

Interviews focused on risk concepts, risk experiences, and how companies manage these risks. We discuss these practices in terms of strategic planning, information management, regulatory risk, and decision-making processes.

More Corporate Emphasis on Strategic Planning

As China’s political economy has changed, especially since Xi Jinping’s ascent and, for example, the launch of Made in China 2025, many companies have initiated discussions on competing in China and what they hope to achieve through China engagements (or a lack thereof) with a broader scope and at higher levels of their organizations. Some of this planning takes shape within working groups on China with personnel who span business divisions and corporate roles, for example, drawing from government affairs, legal, management, and even product divisions. These groups universally seem to sit in corporate headquarters and never in China-based offices.

More broadly, given general concerns about geopolitics after Russia’s invasion of Ukraine, transatlantic tensions over industrial policy, and China, many companies have focused on how to adjust strategy and governance. These efforts include bringing on new board members with foreign policy and national security experience, changing government affairs offices and personnel from primarily domestically connected and focused individuals (i.e., focused on the United States) to individuals with security and foreign policy experiences, and even designating “foreign policy” strategy officers with portfolios for long-term planning to address geopolitical eventualities, including changes to global alliances and regional balance of power issues.

Several company representatives relayed in surveys and in interviews that their firms have established new strategic initiatives in response to geopolitical risks. These include geopolitical risk working groups reporting quarterly to boards and/or management, expanding geopolitical risk in the overall enterprise risk management function, and scenario planning exercises. Overall, these efforts are commendable, but gaps exist in how well integrated they are in comprehensive planning.

Several company representatives expressed frustration that boards and management invite consultants, scenario planning, and high-level discussion on geopolitical and political risk in the immediate aftermath of a global event (e.g., Russia’s invasion of Ukraine, People’s Liberation Army (PLA) exercises after Speaker Nancy Pelosi’s Taiwan visit), but, as one interlocutor put it, “The talk doesn’t seem to move the needle on having strategies that are prudent and proactive rather than reactive.”

Overhauling Decision-Making Processes

As mentioned, many firms have established high-level China working groups, but the groups range in their decision-making function. Many companies have special personnel in government affairs, legal, and/or compliance offices within the firm who undertake significant review and due diligence for China-related activities, but these positions are idiosyncratic and depend on the knowledge of specific personnel. For example, one financial services firm has a due diligence process run by someone with deep China knowledge who conducts reviews of China-related transactions with a sophisticated approach: “If [a Chinese partner] is interested in a certain sector or transaction, we dig very deep to see what PRC government policies are, where the motivation is coming from, how IP in a target firm is organized and held, and what assets—however wild the scenario may be—could be potentially weaponized, even if we are nowhere close to U.S. government lists of restricted sectors.” That individual also said, “We have 35 [U.S.] states with ‘baby CFIUS’ laws or processes, and sophisticated firms have these intense review processes because we want to pass potential government scrutiny and ensure compliance. I feel that we are running a ‘block and tackle’ that allows us to understand some of China’s strategy and also play a role [in ensuring national security].”



Increased Firm-Wide Information Collection and Dissemination Strategies

On the firm side, it appears to be a complicated task to collect signals of threats, including tea invitations, MSS visits, informal pressures, and so forth, and also to assess and track comprehensively how firm actions may affect or be affected by relationships in and with China. Key issues also include the business actions of China affiliates, including whether affiliates have relationships with sanctioned entities inside and outside China. One firm discovered such relationships through a whistleblower and conducted an investigation into its affiliates' entire supply chains to ensure trade compliance, but the concern was that this information was discovered ad hoc without a clear process through which such discovery could be regularized. Firms that self-identify as geographically "sprawling" or with exceptionally diverse business divisions or product lines expressed concern that they often do not know when parts of the firm may encounter China-related risks, for example, launching software updates that violate U.S. or Chinese data laws or marketing efforts that may involve sanctioned entities.

Increased Engagement with the U.S. Government on Regulatory Risk

Managing information related to China's overall political economy and the U.S. government's policies and conceptualizations of China and national security risk presents another set of challenges and opportunities. The legal processes related to U.S. national security concerns are clear (e.g., CFIUS review, export controls), but firms have varying levels of understanding and communication regarding "economic security" and/or what sectors eventually may be designated as "critical and emerging technology" or "critical infrastructure." Many firms, especially high-profile ones, stated they have good relationships with key actors in the U.S. government executive and legislative branches, but smaller firms do not, and even those that do expressed hopes that they could have clearer channels of communication with parts of the U.S. government without fear of political repercussions.

"My number one wish list item would be a secure channel of communication with the national security or intelligence community. I see things happening with our work in China I need help understanding, but I don't want it politicized. I want the U.S. government to know we are serious about addressing national security concerns, but I have no way of showing that, and doing better, without exposing us to reputational issues."

—A senior executive at a high-profile technology and manufacturing company



Increased Compliance Efforts and Resources

Firms have devoted significant resources to compliance efforts in response to sanctions on Russia and have amplified export controls, outbound controls, and other regulatory measures described in the appendix. In interviews, we learned that companies long engaged in dual use or “critical and emerging technologies” have made use of existing compliance regimes. Similarly, financial services firms with committees that scrutinize work for anti-money laundering, Foreign Corrupt Practices Act compliance, and various international entity listings have also repurposed existing firm structures to expand scrutiny for their work in China, especially in response to executive orders prohibiting investment in PLA-related entities. Companies without such structures, especially small firms and start-ups with focus in emerging technologies, have sometimes scrambled to understand the regulatory landscape and ensure that their business practices are designed with compliance concerns in mind. To be clear, no firms expressed difficulty in complying with state and federal regulations, but many, if not most, expressed frustration with reconfiguring practices to anticipate future compliance needs.

The emergence of data- and technology-driven intermediaries is a promising area of innovation in aiding companies with both compliance (due diligence) and threat prevention (especially in supply chain and cybersecurity). In interviews, several companies, large and small, were encouraged by the proliferation of “supply chain risk management” information and analysis provision and “cyber supply chain risk management” mechanisms for due diligence and forensic analysis of software and hardware supply chains. Tools developed by the private sector allow firms to map supply chains, identify potential vulnerabilities, and better know customers and suppliers in the context of entity listings, sanctions, and legislation such as the Foreign Corrupt Practices and Uyghur Forced Labor Prevention Acts. Examples of these tools are in Annex III.

These foregoing categories of responses reflect a corporate sector that takes seriously the new geopolitical landscape and specific dynamics in the Chinese business environment. Nonetheless, companies have had to react to changes in the Chinese, U.S., and global environment often with little warning and at times with limited information about how competition and policy in specific sectors might evolve. Moreover, many of the most sophisticated responses to risk we describe are a result of idiosyncratic or ad hoc experiences and are not designed carefully to detect, manage, and mitigate future threats. We therefore propose an integrated decision-making framework to address these risks in a comprehensive way.

III. Toward a Sustainable Decision-Making Framework to Address Geopolitical Risk

The previous section established that U.S. businesses devote more resources to focusing on geopolitical risk, with much of that effort focused on China. Notwithstanding that most U.S. survey respondents see China as a source of growing concern—with a diverse set of issues underlying that concern—many do not view conducting business in China as discretionary, particularly those whose businesses are outside the scope of national security concerns. They must be in China for manufacturing (to be close to customers); to have insight into the market for commodities and consumer behavior; and/or to tap into the talent in the market and keep up technologically with other global competitors. For these companies, backing away from China is not an option absent some external catalyst.

Engagement with China is, therefore, a rapidly intensifying risk management exercise and one with substantial challenges. For one, the risk mitigation behavior of companies is inconsistent. For example, respondents to the survey noted their concerns with China included threats to personnel, networks, and systems—and specifically to protecting sensitive data and company IP—yet only a minority of firms have undertaken any structural separation to safeguard against such risks. Some respondents also identified China as an important market because of competition they faced at home, yet they also expressed concern regarding the risk to their IP by conducting business in China.

As these responses indicate, part of the inherent challenge with managing China-related risk is that conducting business in China entails systemic conflict. Companies must address political risks in China and beyond China but are also exposed to substantial commercial risks that are sometimes, but not always, related to politics. China is often an attractive market for initial investment. As Chinese businesses become more competitive in a given sector, however, foreign participants can be squeezed out of the market locally and then face competitive risks globally. Equally, as noted, companies need to be near their customers, which include multinationals doing business in China, yet a presence in China also potentially entails greater risk to their IP and personnel.

Legal challenges also exist. Chinese laws, particularly in the national security space, are broadly scoped and not underpinned by a transparent, independent legal system with guarantees for due process as well as meaningful judicial and administrative review. Rather, they are drafted to provide political, intelligence, and state security services with flexibility to control and manipulate the application of these laws and create leverage over citizens and participants in the market. It is inherent to the nature of such services that a business cannot always detect what they are doing, and there are limits to what a business can do to defend against this.

Finally, companies also have a comparative information and resource deficit. As increasingly rich as data have become for companies, that richness pales in comparison to the information and resources available to a government—particularly an authoritarian government that exercises control throughout the country.

The experience of the LED (light-emitting diode) industry is instructive. Starting in the early part of the 2010s, Chinese entities, with substantial funding from the government, began to buy large volumes of metal organic chemical vapor deposition (MOCVD) tools. MOCVD tools are used to grow crystalline layers to create semiconductor multilayer structures. Essentially, an MOCVD is a complex machine to make the foundational wafers for semiconductors or LEDs. For a country like China that sought to be a global technology player, it was natural as a matter of economic policy to have an interest in MOCVD machines. The best way to have a strong technology sector is to develop a strong semiconductor industry, which can spawn adjacent innovation. LEDs are a close cousin to semiconductors.

Chinese companies bought these MOCVD tools in substantial volumes, saturating the market and lowering the cost of production, which then incentivized other companies to move production.¹⁴ China also subsidized domestic champions, helping them compete globally. In parallel, it undertook a campaign to acquire certain key foundational technology abroad.¹⁵ For commercial makers of LEDs—and a company that sold the machines—it seemed like there were valid commercial reasons to be attracted to the market given the volume of government resources into the market.¹⁶

But the economy was not the Chinese government's sole motivation. LEDs often are based on gallium nitride (GaN), not silicon, and GaN epitaxy, which MOCVDs produce, can have a power effect that has significant military and commercial applications.¹⁷

The physics and processes behind growing GaN for the flashlight on a phone or car headlights are not too far off from the physics to grow GaN for lasers, radars, directed energy, 5G, and exascale computing (necessary to run the calculations to maintain a nuclear deterrent capability in a comprehensive test ban treaty world). The focus on LEDs was not simply commercial; it was part of a military-civil fusion policy.

In 2015 and 2016, LED businesses that had specialized knowledge of growing GaN-based epitaxy started to go on the market, in part because the saturation in manufacturing in China and Chinese government subsidies to Chinese competitors started to squeeze the margins for LED businesses in the West. Not surprisingly, there was considerable Chinese interest in acquiring these LED companies with investment from Chinese government-owned investors funding the bids, and the business thesis was clear: Acquire the business with the know-how to make good LEDs, move that capability to China to take advantage of the lower-cost manufacturing, and then substantially larger margins on the business and an exit into a super-charged Chinese public securities market or listing in the West would be remunerative.¹⁸

Before these western LED businesses went on the market, at least one of them experienced a theft of its trade secrets by an employee who then relocated to China and worked for a Chinese competitor.¹⁹ Later, in a separate effort to obtain technical know-how, one of the large Chinese LED companies, which was heavily subsidized by the Chinese government, canceled a huge order of MOCVDs from the German company Aixtron, one of the principal manufacturers of MOCVDs, which resulted in a 43% decline in its share price and put the company on weak footing. Some months later, a separate firm with investor connections to the Chinese customer that canceled the orders approached Aixtron with a bid at a sizeable premium over its share price.²⁰

¹⁴ <https://www.semiconductor-today.com/features/PDF/Semiconductor%20Today%20-%20MOCVD%200911.pdf>

¹⁵ https://www.ledinside.com/news/2013/11/chinese_mocvd_equipment_manufacturers_to_challenge_top_foreign_brands

¹⁶ <https://sst.semiconductor-digest.com/2012/02/aixtron-mocvd-tools-easier-to-lease-in-china-with-new-msfl-alliance/>

¹⁷ <https://semiengineering.com/mocvd-vendors-eye-new-apps/>

¹⁸ https://www.ledinside.com/showreport/2017/5/global_lighting_companies_market_strategies_in_the_post_led_lighting_era

¹⁹ <https://www.digitalguardian.com/blog/semiconductor-company-awarded-66m-trade-secret-theft-case>

²⁰ <https://merics.org/en/report/made-china-2025>



Aixtron agreed to the deal. CFIUS, however, obtained a presidential order prohibiting the transaction in the United States, but first the U.S. government briefed the German government, which pulled back its approval of the deal citing concerns about how it could help the Chinese nuclear program.²¹

Thus, China used government subsidies to alter the market dynamics for LED producers, creating a gravitational pull to put manufacturing in China. In parallel, Chinese firms undertook separate actions, including IP theft and proposed global acquisitions at inflated prices, to complement the manufacturing capabilities. It is unlikely that any of the target western LED businesses understood the full picture of this effort. Each firm owed duties to shareholders to optimize the value in a market where it was becoming harder to compete against Chinese firms, and the locus of manufacturing was shifting to China.

In response to these and other experiences, the U.S. has cast a broader regulatory net on investment and trade issues, but its motivations for doing so are not always transparent to businesses that, in turn, remain at an information deficit. In this context, it is imperative for U.S. businesses to develop their own solutions—solutions that optimize short-, medium, and long-term decision-making by developing a well-informed, holistic, enduring, authoritative, and tailored decision-making framework. To be clear, such a framework should be tailored to the specific business for it to be effective. There is no one-size-fits-all model, but common elements are as follows.

²¹ <https://www.reuters.com/article/business/germany-stalls-chinese-takeover-of-aixtron-citing-security-worries-idUSKCN12013F/>; <https://www.nytimes.com/2016/10/25/business/dealbook/germany-china-technology-takeover.html>; <https://phys.org/news/2016-10-chinese-takeover-german-firm.html>



Box 3.1: Principles of a Decision-Making Framework

WELL INFORMED

A well informed decision-making framework should have a governance committee with participation by individuals with knowledge of China and/or the company's motives for engagement in or with China. To further ensure that the committee's decisions are well informed, the firm should have a coherent and documented strategy for China engagements as well as a means of periodically collecting and reviewing new information as it pertains to both company engagements in and with China and relevant changes in China's landscape.

HOLISTIC

The governance committee should have a whole-of-enterprise view of political and commercial risk as it pertains to engagement in and with China. We recommend, therefore, that the governance committee have inputs from business units but sit at the management level with reporting to the top of the company (CEO, board, investment committee) as appropriate.

ENDURING

The process of governing engagement in China should be institutionalized within highly exposed firms. As noted, governance should be organized in a committee that has a clear and transparent process and is designed to last beyond personnel and strategy changes for the lifetime of China engagement or exposure.

AUTHORITATIVE

A governance committee should have clear decision-making power over business activities that are affected by or affect China engagement or exposure.

TAILORED

The staffing, process, and function of the committee should be adapted to fit the company's business units and needs.

Governance

A sound decision-making framework starts with a clear governance model, such as forming a geopolitical risk management committee. For most organizations, this will be organized at the senior management level to inform the policy and decision-making of the organization, including the board.²² It should include management-level representatives who will be able to reflect a holistic view of the organization, for example, relevant business, legal, security (including IT), and enterprise risk management personnel. The committee should be tailored to the organization but would generally be appointed and empowered by the highest levels within the organization (e.g., the board or senior management) and report to the same.²³ This committee, in turn, should define what decisions it will review and on which it will provide direction; that is, it should define what business activities are covered in the committee's purview. Examples include the following:

- Existing footprint, operations, and investments in the PRC
- Investments in PRC entities that involve any acquisition of equity or debt, regardless of size or joint R&D with PRC entities
- Material staffing developments in China²⁴
- Taking on specific projects or clients with PRC entities
- Establishing new operations in the PRC

- Integration or separation of assets and personnel in the PRC with the rest of the world
- Commercial sales or opportunities with PRC entities or otherwise in the PRC, to be defined with more specificity (based on size and possibly criteria based on sensitivity of IP, counterparty, etc.)
- Supply chain, with a focus on preexisting and emerging dependencies for critical inputs for the business

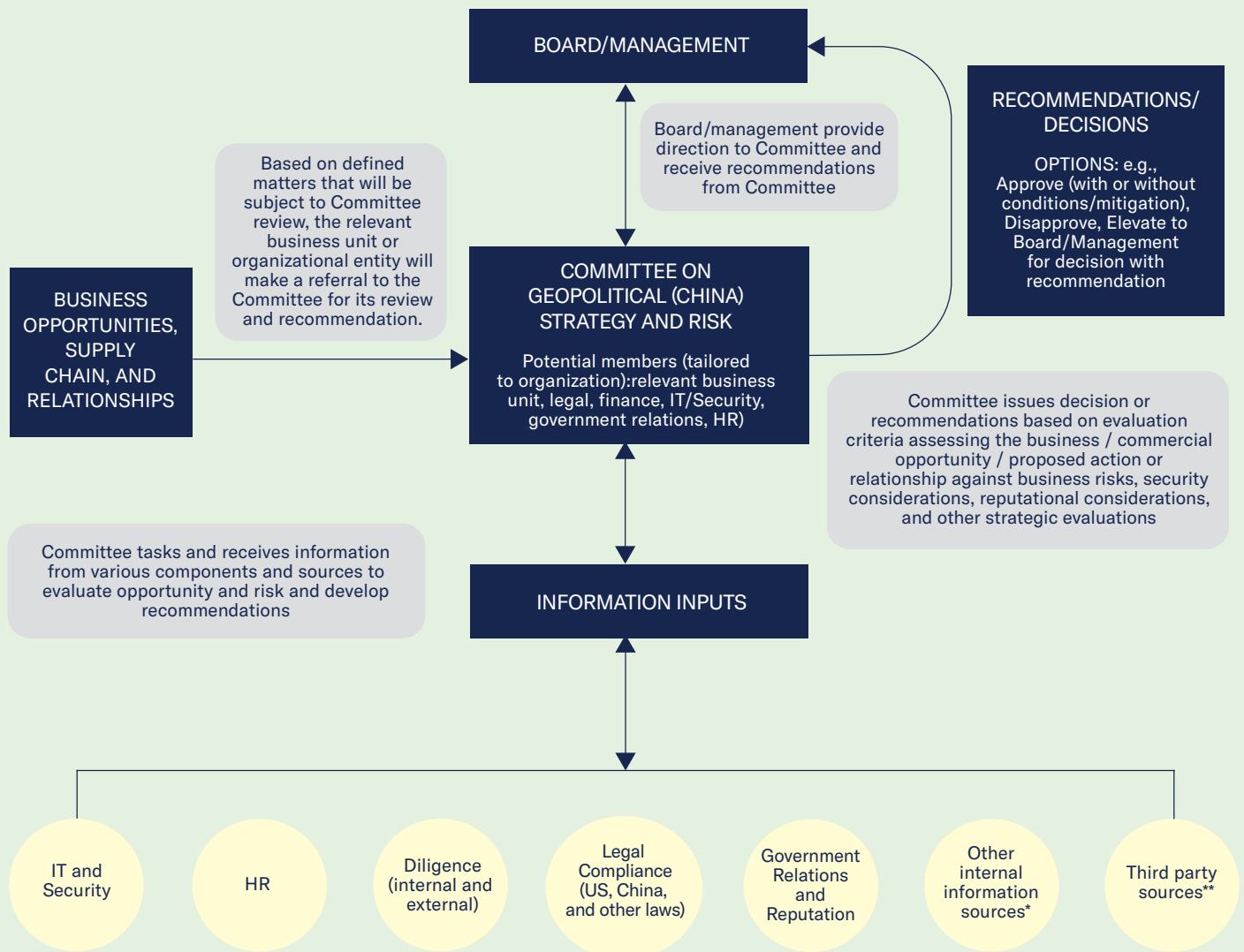
For decisions that are elevated to the committee, the committee would also be charged with approving and overseeing requests for further information and, in certain cases, development of mitigation strategies. Figure 3.1 represents how such a framework, subject to tailoring based on firm structure, might receive inputs and how decision-making might flow.

²² Organizations with a high degree of exposure to China and tensions between the United States and China may also wish to include expertise on risk management and geopolitical issues in some capacity on its board.

²³ The committee should be organized and report up in a way that makes sense for the firm. For some firms, a risk governance committee would report to the CEO, and in others, it would report to the CEO and board. Still others may be organized differently. For example, private equity firms would have risk committees report to the investment committee.

²⁴ This is an issue for multinational companies doing business in China because it has become harder to sustain expatriate presence in management and leadership, and local laws and business press businesses to have a more Chinese-focused style of operations. As discussed in the "process" section, there is no clear right or wrong approach, but this type of staffing decision—moving to a more domestic presence in their management and operations—is arising for businesses and presents both opportunities and challenges.

Figure 3.1: Geopolitical Risk Governance Framework



* Important to track relevant data across organization so that it can be leveraged for decision

** Includes open source or other publicly available information, third party diligence, or government information inputs

Process

The committee should also define and develop a process for those decisions and opportunities that will be presented to it. Consistent with the notion that such a structure should be tailored to the organization, it is optimal to start with the business lines that are most affected by China and/or have the greatest opportunities with China to develop the information and criteria to present to the committee for decisions. This may include inputs from the business team in China and from business units based outside of China. Once the business presentation is received, inputs from legal, security (including IT), and other relevant functions (human resources, enterprise risk, etc.) can be added. For many organizations, the business unit, with information inputs from legal, security, and other relevant functions, then will be responsible for presenting the full package to the risk management committee. At this point, the committee will have the options to approve, approve with mitigation conditions, reject the requested approach, or require more information.

Criteria for Decisions

The criteria for a governance committee decision should take into consideration all relevant factors and information. The business considerations will be highly contextual to the business and the specific opportunity at hand. The legal considerations, however, can be more readily identified. They will include traditional commercial legal considerations for the particular relationship (whether commercial, vendor supply, investment, etc.) and regulatory considerations. From a U.S. law standpoint, these may include investment-related regulations (CFIUS or outbound regulations, depending on the nature of the transaction and sector at issue); compliance with U.S. trade controls laws (export controls and sanctions); compliance with the Uyghur Forced Labor Protection Act for certain supply relationships; and other compliance-related considerations, as applicable (e.g., for government contractors, compliance with certain supply chain requirements).

Equally, there should be a consideration of China-related legal implications. These may include the extent to which the contemplated business relationship implicates Chinese data and cybersecurity laws; whether it is a transaction that requires approval of Chinese authorities; whether it involves Chinese-origin technology that could be subject to Chinese export control laws; and, importantly, whether the activities at issue include conduct within China that could be of interest to, or a concern for, the Chinese state security services (e.g., implicate obtaining information that China would not want exported or accessible to non-Chinese parties).

In addition to the United States and China, other countries' legal considerations may also be relevant depending on the business conduct or opportunity at issue. For example, if a transaction with China involves U.S. origin technology that also is developed and supplied through a third country, then, in addition to U.S. export control laws, the third country's other export control laws may be relevant. In addition, some companies may find that investments or activities in third countries (i.e., neither the United States nor China) may be affected by or affect overall China strategy and exposure. In those cases, the governance committee may expand its process to cover such transactions as part of a holistic review.

From a security standpoint, the governance committee should assess a range of considerations. These include (1) protections of company data and systems outside of China (e.g., through network segmentation and strict access controls), (2) protections of company data and systems within China, (3) an evaluation of risks to company personnel in China and traveling to China, and (4) insider threat risks.

Developing a Holistic View of Risk and Mitigation

As noted, the objective of the foregoing risk management framework is to develop a mechanism that has institutionalized endurance and authority. To do so effectively requires robust information inputs—information inputs that can provide a more holistic view of risk and potential mitigations. This is an all-source analysis that should leverage publicly available information and proprietary databases and services that can provide deeper insights into beneficial ownership and trends and developments in China, internal intelligence from security teams, tracking cyberthreat activity, documenting and tracking other forms of suspicious activity reporting (e.g., employees being taken to “tea” in China, temporary exit bans, approaches to employees via social media or cold-call emails), and other threat reporting. Although it has become more challenging to conduct on-the-ground diligence in China, third-party diligence providers can still provide insight and analysis through information collected remotely.

In addition, businesses should conduct scenario planning exercises and leverage the lessons from those exercises to inform their governance considerations and criteria as well as keep track of changes in Chinese and U.S. (and other) laws, interpretations, and enforcement.

Maintaining and periodically reviewing such all-source information is critical to identifying and making connections between various threats and, in turn, devising risk mitigation strategies. For example, if operations in China will interact with employees in the United States who have access to highly sensitive customer data and proprietary IP, then various mitigation strategies—including training for the U.S. employees on information security and insider threats, implementation of network segmentation, and clean device policies for U.S. employees to travel to China—can be implemented to reduce the risk exposure.

Evaluation criteria also should include an assessment of reputational risks. Such an assessment may include, for example, (1) the ownership and profile of China-based counterparties (e.g., there may be higher risks of Chinese counterparties who are on certain trade controls or sanctions lists maintained by the U.S. government); (2) the relationship between China-based counterparties and the PRC government, the People’s Liberation Army, and/or PRC state-owned entities; and (3) an assessment of the nexus, if any, between the commercial opportunity at issue and any PRC state military, defense, or intelligence interests. These reputational considerations may affect relationships with customers and counterparties outside of China as well as increase certain public relations and legal risks, such as the risk of Congressional investigations.

Finally, it is worth noting that the foregoing may apply even to those businesses that do not have a footprint in China. First, businesses in one sector can be subject to retaliatory actions for activities in a completely different sector, regardless of whether they have a presence in China. Second, changes in policy in the United States, China, or even other countries, and quick shifts in the law, may have a substantial impact on business decisions. For example, the auto industry has recently had to grapple with the prospect that sourcing certain components from China—even those developed and controlled by Western firms—may no longer be viable because of the connected vehicle rules of the Department of Commerce.²⁵ This example illustrates the importance for all businesses of being able to track laws, trends, and potential legal developments emerging out of the U.S.-China competition, including those in the criteria and process for decision-making on China-related risk.

²⁵ <https://www.federalregister.gov/documents/2025/01/16/2025-00592/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles>

Applications: Examples

FINANCE

Several financial services firms participated in interviews for this report, and some have developed governance frameworks that apply the principles in Box 3.1. Those firms have experienced more streamlined and better-informed decision-making as it pertains to China, reputational, and commercial risks.

One global investment firm designed an internal risk review team with the goal of systematically reviewing China-related risk. A team of three to five risk professionals with national security, technology, and public policy training or experience reviews every investment decision to screen for national security, reputational, and commercial risk. The company reports that 90% to 95% of transactions reviewed each year present no such risks, but 5% to 10% require more information and due diligence, are permitted with mitigation measures, or are blocked by the internal review committee. Creating the review process was part of the company's broader investment thesis globally and by sector.

For financial services firms generally, risk committees are equipped for screening for Foreign Corrupt Practices Act (FCPA) or anti-money laundering purposes. Moreover, for various firms, including private equity companies with China-based investments or investors (passive investors), due diligence processes were expanded to include evaluating information on China's state industrial strategies (e.g., Made in China 2025, five-year plans, local and provincial policy statements and subsidies), as well as Chinese investor strategies and relationships with competitor firms. Those processes generally resided with legal and compliance officers and demonstrated the promise of intensified screening of China engagements within firms.

TECHNOLOGY

Several major technology firms have established "China working groups" with input from legal counsel, management executives, and government relations personnel. Although most of these working groups were holistic, well informed, and tailored, they were not enduring (institutionalized), nor did they have authority over company decision-making.

One technology firm initiated a process similar to the one described earlier by the investment firm. For this technology company, business units submitted any activity related to China to a review committee for reputational, national security, or commercial risks to a similarly staffed committee. However, the process seemed considerably more challenging than that for the investment firm because the decisions made by business units were more heterogeneous and involved everything from investments to sales decisions to joint marketing projects. Nevertheless, the company reported that the process it developed to evaluate China-related risk helped refine global strategy, streamline compliance with export controls and outbound restrictions, and address reputational concerns in China and the United States.

Scope

The examples on the prior page are from companies with multifaceted exposure to China, meaning they engage with China in more than one of the ways listed in Table 3.1 (see also Section II survey data). We recommend that companies that have multifaceted exposure consider a framework, regardless of industry. Clearly, companies engaged with China sectors that are the focus of military and economic competition between the United States and China (for illustrative lists, companies can reference Made in China 2025 or various lists issued by the U.S. government, such as critical infrastructure, emerging and foundational technologies, critical minerals, aerospace and defense, life sciences, and others) should develop a framework, but we note that definitions and designations are dynamic. For example, various service industries may not fit neatly into sector designations by either country but could still be broadly relevant. Further, sectors not considered of national security relevance now may be considered as such in the future by the United States, China, or both countries, and commercial threats from China's desire to compete in specific sectors can emerge quickly and in ways that are hard to detect. Companies with significant China exposure should have frameworks to anticipate these changes and adjust practices in response.

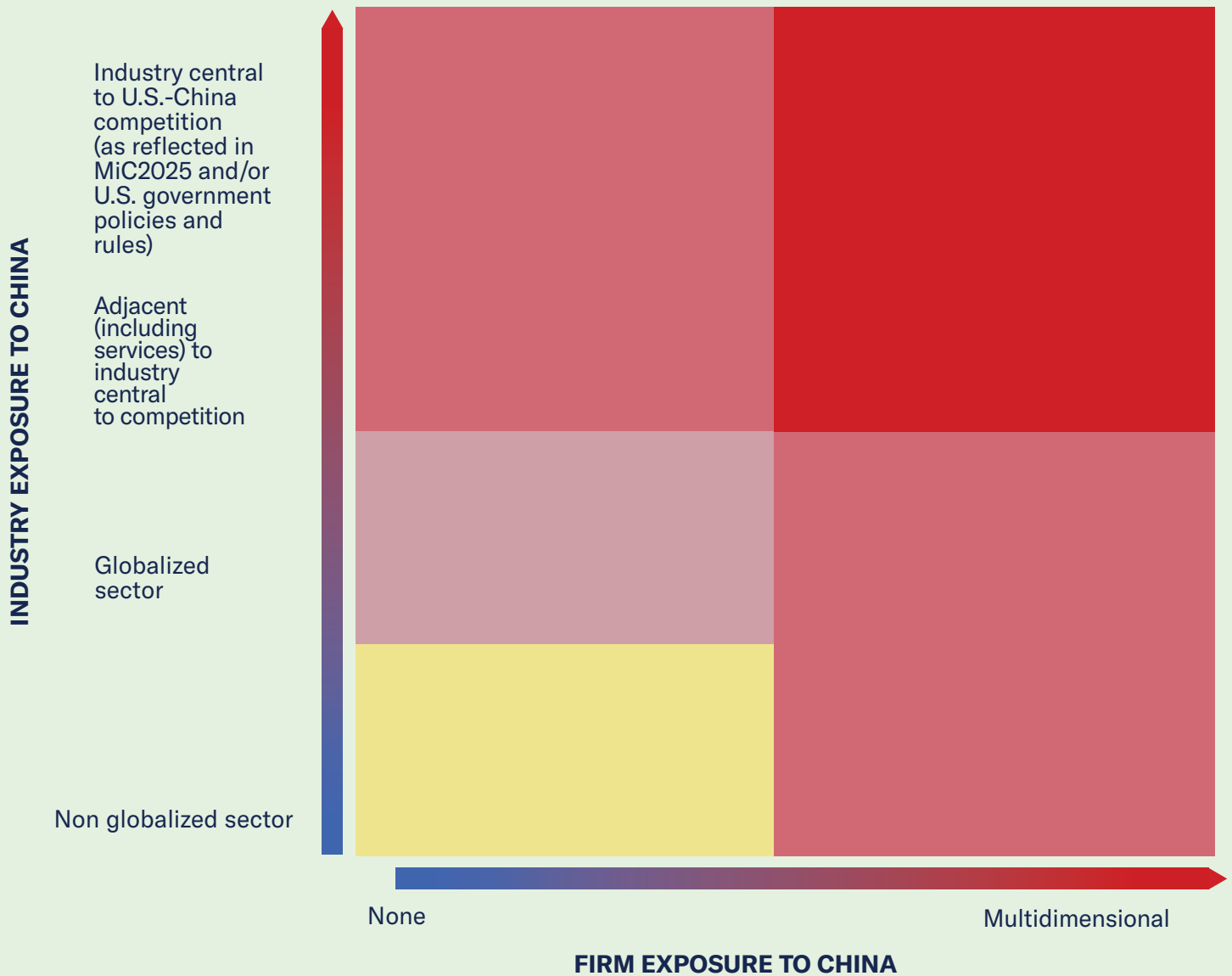
Many companies in the United States have only one dimension of China exposure or perhaps no direct exposure. Such companies may not be in need of as robust a framework as the one outlined here; nevertheless, they will still merit some form of a framework. We learned in interviews and in survey data that many such companies with no direct China exposure focus on information collection related to China because China's industrial strategies and practices in their sectors have profound implications for the overall competitive landscape. Moreover, even companies without direct China exposure may face risks to IP and data or personnel security.

Critically, the centrality to competition is not solely determined by U.S. policies and regulations but also by China's policies and strategic plans. These companies, too, should have well-informed, enduring, holistic, and tailored efforts to assess China's role in their sector and how the U.S.-China competition could affect their activities. Figure 3.2 visualizes the need for a framework (all red boxes) as firms vary in exposure to China by firm and industry.

Table 3.1: Exposure to China

-
- Personnel based in China
 - Sell products in China
 - Competitors based in China
 - Source products or services from China
 - Direct investments in China (including joint ventures)
 - Provide services to China-based companies
 - Conduct R&D in China
 - Investment from China

Figure 3.2: Need for Risk Management Framework by Firm and Industry



Public Benefits of a Geopolitical Risk Management Committee

The primary goal of recommending such a framework is to help companies manage and mitigate commercial and political risks. We are grateful to the companies that spoke with us and to the survey respondents who shared their concerns and best practices. We have offered the governance framework outlined herein as a “best practice” for companies exposed to these risks.

There could be additional benefits for the U.S. business environment and public policy should these practices be adopted more widely. First, a governance framework can focus company knowledge and experiences with political risks on China, providing a clear locus of decision-making within companies that can interact with groups outside companies in productive ways.

For example, in our discussions of technology transfer and organized but hard-to-detect Chinese industrial strategies targeting specific sectors, many companies make decisions, such as investment in or relocation to China, because their competitors pursue similar actions, and the full picture of how China approaches a particular sector is beyond the vision of an individual firm. Having a group of decision-makers within companies focused on this issue may not resolve all of these issues, which are collective action problems by function of competition, but it opens a pathway for horizontal information sharing and best practice adoption that might help.

The same is true for interactions with the U.S. government, especially the U.S. national security and intelligence community. The U.S. government, on the one hand, and businesses engaged in China, on the other, each hold deep and relevant information unavailable to one another. There are real and sensible limits on how much of that information can be shared (e.g., classification, U.S. companies do not want to be seen as agents of U.S. intelligence, protection of trade secrets), but many interviewees expressed a desire for better means of communication with U.S. authorities, and the concentration of focus on China's commercial and strategic actions at least provides a point of contact within firms that might benefit the development of communication.

Industry associations may play a role in this information sharing and best practice dissemination. As outlined in the case of LEDs, China's participation in many sectors presents whole-of-industry threats. We encourage industry associations to develop and disseminate information about China's role for their members and to organize members to tailor decision-making processes and share best practices to resolve collective action problems. Many industry associations already do this. Such associations are particularly well placed to aid members, especially new entrants and companies without significant government relations resources, in adopting prudent practices.

Last, the governance framework we recommend can be made appropriately transparent, or at least legible, to both company stakeholders and legislative and regulatory decision-makers in the United States. There will be limits to what companies can and should share about their internal governance processes, but such a process can fortify trust between policymakers and U.S. companies that will continue to do business in and with China. And, by fostering better decision-making within companies—decision-making that can be informed by a broader survey of risk and, in turn, be more clear-eyed about such risk—a broader adoption of such governance frameworks can also help advance U.S. national security interests.

Annexes

Annex I: China Regulatory and Political Economy Landscape

The relationship between the United States and the PRC has transformed definitively from engagement and economic integration to geopolitical competition. The structure of that competition, evident in changes in the policy environments in China and the United States, affects businesses of all kinds, not just those engaged directly or even indirectly with the Chinese market. Firms are exposed to geopolitical competition through China's domestic policies to reshape the economic environment, a reconfigured landscape in the United States targeting security concerns in economic engagement with China, and China's retaliatory responses. Broadly, the contours of geopolitical competition are undeniably economic, as China has pursued "comprehensive national security" through advancement in technology and dominance in critical global supply chains. Businesses making commercial choices in China and elsewhere must reckon with China's national strategies as well as U.S. responses and must address the national security externalities of their actions and the strategic and commercial risks that geopolitical competition presents.

The Chinese political economy has changed drastically in the past decade in a way that has both exacerbated previous challenges and presented novel ones for foreign business and for foreign governments whose firms are engaged in and with the Chinese system. Common challenges long associated with China's system have included frustrations about market access and what U.S. firms and policymakers deem a lack of "fair competition" with Chinese firms. In this period, concerns have intensified under the government of Xi Jinping (2013 to present) regarding the security orientation of the Chinese state and economy, which is manifest in industrial policies like Made in China 2025, civil-military fusion efforts, a suite of laws and regulations that give the state broad authority to intervene in firm activity, and a general posture of technological and security competition. In this context, economic interdependence with China, once viewed as a ballast for the U.S.-China relationship and a source of mutual, even global, prosperity and security, has itself become the site of pronounced security concerns for the United States and other governments alike.²⁶

²⁶ Margaret M. Pearson, Meg Rithmire, and Kellee Tsai. 2022. "China's Party-State Capitalism and International Backlash: From Interdependence to Insecurity." *International Security*, 47(2): 135-176.

Military-Civil Fusion

Beijing's efforts at military-civil fusion (MCF) have expanded in scope and degree under Xi Jinping, with broader efforts at advancing the technological power of the People's Liberation Army (PLA) by breaking down barriers between academic and economic innovation and China's armed forces. The shift from a milder "civil-military integration," the language of the 1990s and early 2000s, to MCF began under Hu Jintao and has accelerated under Xi.²⁷ In particular, the 13th Five-Year Special Plan for Science and Technology Military-Civil Fusion, issued in 2015, called for "integrated development of economic construction and national defense construction."²⁸ In implementation, the plan aims to involve universities, research institutes, and firms of all kinds of ownership in military upgrading efforts through R&D, commercialization of technology, and logistics.

The MCF goals are ambitious. Some researchers urge caution in assuming the strategy is a "fait accompli," emphasizing the low levels of participation in military modernization on the part of nonstate firms in China and the considerable challenges of integrating China's high-tech sector with the PLA, even with considerable financial resources at play.²⁹ Others have viewed MCF efforts with serious alarm, documenting organized efforts to acquire advanced technological capabilities for the PLA by emboldening government access to private data and technology, forcing involuntary participation from firms in China, providing government support for strategic industries, and leveraging the PRC legal regime to extract compliance.³⁰

The extension of the PLA's potential reach, and substantial concern on the part of U.S. and global policymakers that global firms will work with Chinese firms that end up aiding in China's military modernization, requires firms engaged in or with China to apply extra scrutiny to their business partners and activities.³¹ Put simply, the assets and actions of firms are central to the PRC's efforts to acquire capabilities in the military and national security realm. China's global security posture and efforts at MCF have driven foreign governments, including the United States, to more tightly regulate outbound technology flows to China and to covered Chinese persons that have dual-use application and could support China's military, intelligence, and domestic security services (see Annex II on the U.S. Legal and Regulatory Landscape).

²⁷ <https://www.csis.org/blogs/trustee-china-hand/chinas-evolving-conception-civil-military-collaboration>

²⁸ http://www.xinhuanet.com/politics/2016-07/21/c_1119259282.htm

²⁹ <https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy>

³⁰ <http://jamestown.org/program/civil-military-fusion-and-the-plas-pursuit-of-dominance-in-emerging-technologies/>. See also U.S. Chamber of Commerce China Center. A Primer on China's Military-Civil Fusion Strategy for American Business: Risks, Compliance, and other Implications. April 2020. <https://ucigcc.org/publication/chinas-fortress-economy/>

³¹ <https://www.uscc.gov/hearings/us-investment-chinas-capital-markets-and-military-industrial-complex>

Indigenous Innovation

China's weak intellectual property protection has long been a problem for firms engaged there, but a marked shift has occurred from copying—trademark infringement, copyright violations, and so forth—to a more sophisticated regime of policies aimed at domestic upgrading and indigenous innovation at the expense of foreign firms. The Chinese government's efforts to push domestic firms to upgrade present an array of risks for U.S. firms because these efforts are present at various levels of government and through both formal and informal policy channels. These efforts may be hard to detect and furthermore rely on global firms making individual commercial choices that, in the aggregate and over time, can result in empowering Chinese competitors and critical dependencies on the Chinese market.

Technology transfer: Multinational firms competing in the Chinese market were, until the 1990s in some sectors and following WTO accession in others, required to partner with a Chinese domestic firm (joint venture), and many of these arrangements entailed transfer of technology (ToT) stipulations, by which global firms agreed to formally transfer IP, sometimes even training Chinese domestic firm personnel.³² In other cases, ToT requirements have been a condition of accessing the Chinese market, especially in “strategic” sectors such as telecommunications, infrastructure, information technology, and energy or power generation and transmission. A 2023 analysis found that technology extraction efforts, including joint venture ownership, local content, and preferential public procurement policies, increased sixfold (from 53 to 339) in the decade after WTO accession, and they were most common in industries in which foreign firms rely on the Chinese market to sell finished goods.³³

ToT efforts present a thorny challenge to global firms. If they resist ToT pressures, they risk losing access to the Chinese market (in terms of both market share and China as a production base). Moreover, their competitors may nonetheless agree to the ToT conditions, which would enable Chinese firms to upgrade and their competitors to grow market share and/or increase production efficiencies, challenging their positions globally. In addition, many firms that agree to ToT, even for “last generation” technology or when their Chinese competitors were embryonic, find themselves eventually edged out by those Chinese competitors in China and abroad. ToT policies, therefore, present both a temporal and a collective action problem for multinational firms: What is beneficial to the company at one moment may later be cause for regret, and individual companies face challenges in refusing ToT if their competitors will not do so.

Accelerating domestic upgrading after WTO: China's overall efforts at domestic upgrading have accelerated at a policy level since WTO accession. Changing national policies as well as China's fragmented local bureaucracy challenge efforts to identify specific policies to pursue resolution at a diplomatic level or calculate risk for companies. Diplomatic channels have included Strategic and Economic Dialogues, U.S.-China Joint Commission on Commerce and Trade, and discussions about a Phase One Trade Agreement in 2020, but domestic rules on patents, standards, competition, and procurement mandates have enabled the PRC government to pursue domestic preferencing despite international commitments and rhetorical agreements in these nonbinding dialogues.³⁴

³² Margaret Pearson. 1992. *Joint Ventures in the People's Republic of China: The Control of Foreign Direct Investment Under Socialism*. Princeton: Princeton University Press.

³³ John David Minnich. 2023. “Scaling the Commanding Heights: The Logic of Technology Transfer Policy in a Rising China.” <https://scee.fsi.stanford.edu/china-briefs/assessing-strengths-and-limitations-chinas-technology-transfer-policies>

³⁴ <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/november/us-fact-sheet-27th-us-china-joint>

At the national level, early 2000s emphasis on “indigenous innovation” coalesced into the State Council’s 2006 “**National Medium- and Long-Term Plan for the Development of Science and Technology**” (MLP), which set targets for R&D expenditure (2.5% of GDP), the contribution of science and technology to economic growth (60%), and reduction of dependence on foreign technology (to below 30%).³⁵ Policy implementation varied, but local governments competed for recognition in their efforts to encourage indigenous innovation and technological development, often requiring multinational firms to source locally and transfer technology and granting significant subsidies to local firms.³⁶ Many of the state’s efforts to develop advanced technologies channeled resources to large, state-owned firms that were often inefficient and uncompetitive relative to both international firms and domestic private firms. As a result, many of China’s innovation policies were dismissed as targeting “paper tigers” that would not challenge the positions of international players,³⁷ but the direction changed with the Strategic Emerging Industries (SEI) program in 2010. Like the MLP, the SEI championed technology-intensive industrial policies but pursued market creation (i.e., demand side, market-making strategies) for frontier and emerging industries rather than domestic innovation of extant technology. The SEI program also entailed a much larger “resource flow” than the MLP.³⁸

Made in China 2025: The MLP and SEI programs were both rooted in anxieties on the part of China’s leadership that the country’s economy would be stuck with low value-add industries or activities and vulnerable to stoppages in foreign technology. The same anxieties drove the Xi Jinping administration to pursue China’s most ambitious industrial policy in the reform era, Made in China 2025 (MiC2025), which launched in 2015. MiC2025 targets the same sectors as the SEI program (see Table A1.1 in the appendix), with a model of state-led investment similar to venture capital or private equity with nonstate firms both managing the funds and eligible for seed capital from those funds. Determining the amount of funding to the target sectors is difficult, because funds are often announced with target amounts of capital in hopes that private investors will follow the state’s “steerage,” but estimates suggest that more than 11 trillion RMB flowed into firms in targeted sectors by 2021.³⁹

³⁵ See also https://www.uschamber.com/assets/archived/images/024001_us_china_decoupling_report_fin.pdf#:~:text=The%20U.S.%20Chamber%20of%20Commerce%E2%80%99s%20China%20Center%20has.

³⁶ Ling Chen, 2018. *Manipulating Globalization: The Influence of Bureaucrats on Business in China*. Stanford University Press.

³⁷ Douglas Fuller, 2016. *Paper Tigers, Hidden Dragons: Firms and the Political Economy of China’s Technological Development*. Cambridge University Press.

³⁸ Barry Naughton, 2021. *The Rise of China’s Industrial Policy, 1978–2020*. Mexico: Universidad Nacional Autonómica de México. Chapter 3.

³⁹ Barry Naughton, 2021. *The Rise of China’s Industrial Policy, 1978–2020*. Mexico: Universidad Nacional Autonómica de México, p. 106.

Table A1.1: Industries Targeted in China's Domestic Innovation Plans

Medium- and Long-Term Plan for the Development of Science and Technology (2006)	Strategic and Emerging Industries (2010)	Made in China 2025 (2015)
<p>Core electronics, software, chips</p> <p>Manufacturing technology</p> <p>Next-generation wireless communications</p> <p>Precision machinery</p> <p>Oil and gas extraction</p> <p>PWR and high-temp nuclear</p> <p>Water pollution control and treatment</p> <p>GMO breeding</p> <p>Pharma</p> <p>Infectious diseases treatments and vaccines</p> <p>High-resolution satellites</p> <p>Large passenger aircraft</p> <p>Space exploration</p> <p>Shenguang ICF</p> <p>Beidou navigation</p> <p>Hypersonic technology vehicle</p>	<p>Energy conservation and environmental protection</p> <p>Energy-efficient machinery</p> <p>Environmental protection</p> <p>Recycling and reutilization</p> <p>Next-generation IT</p> <p>Next-generation internet</p> <p>Core electronic components</p> <p>High-end software and information services</p> <p>Biotechnology</p> <p>Biopharma</p> <p>Biomedical engineering</p> <p>Biological agriculture</p> <p>Biomanufacturing industry</p> <p>Precision and high-end machinery</p> <p>Commercial aircraft</p> <p>Satellites and applications</p> <p>Railroad and transport machinery</p> <p>Marine engineering equipment</p> <p>Intelligent manufacturing equipment</p> <p>New energy</p> <p>Wind power</p> <p>Solar power</p> <p>Biomass energy</p> <p>New materials</p> <p>New energy vehicles</p>	<p>Information technology</p> <p>New energy vehicles</p> <p>Robotics</p> <p>Aerospace</p> <p>Rail transportation</p> <p>Oceanographic engineering</p> <p>Agricultural machinery</p> <p>New materials</p> <p>Biopharmaceuticals</p> <p>Digital machine controls</p>

Sources: China Medium- and Long-Term Plan for the Development of Science and Technology (2006), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf ; State Council Decision on Encouraging the Development Strategic and Emerging Industries (2010). Chinese: https://www.gov.cn/zwgk/2010-10/18/content_1724848.htm; <https://merics.org/en/report/made-china-2025>.

MiC2025 generated backlash globally from regulators and policymakers in countries, like the United States, with advanced sectors in targeted industries. Because MiC2025 encouraged Chinese investment consortia to look abroad for acquisition opportunities, a pattern of high-technology investment in the United States and elsewhere triggered scrutiny (see Annex II on the United States). The suffusion of state capital throughout the Chinese economy, including in nonstate firms, also makes partnership with and investment in companies in advanced sectors in China potentially problematic for global firms. MiC2025 has been accompanied by renewed and redoubled efforts to offer preferential policies to domestic firms, including increasingly restrictive domestic procurement guidelines. These efforts are often relayed in language that emphasizes the need for China's economy to be resilient to "extreme situations," including war, and for self-reliance.⁴⁰ State firms and government offices in China, much like their global counterparts, voice growing concerns about the ownership and production base of the supplies they source, including informal and formal preferences for local providers and stringent, exclusionary security criteria for vendors.⁴¹ Although many global firms have addressed these policies by localizing production ("in China for China") and/or segmenting production systems, the direction of policy toward domestic suppliers does not preclude a future in which any foreign-owned company might face exclusion from the Chinese market in key sectors.

Last, the tremendous flow of resources into targeted sectors, coupled with political imperatives for local governments to nurture firms in those sectors, has resulted in **overcapacity** with global implications. China's model of industrial policy is investment driven; competition is often fierce among firms within China as sectors are targeted with subsidies and state investment, and waves of overcapacity in globalized sectors shape markets and prices for firms, even those with no direct activities with China. In 2024, Jay Shambaugh, undersecretary for International Affairs at the U.S. Treasury Department, projected that the Chinese supply of battery power would be double world demand by 2027, solar supply would be nearly triple world demand by the end of 2025, and Chinese electric vehicle production would exceed global demand by half by 2030. He concluded that "these features of China's economy can lead to industrial overcapacity that has significant spillovers around the world and can compromise our collective supply chain resilience given the resulting overconcentration in some manufacturing sectors."⁴²

⁴⁰ <https://ucigcc.org/publication/chinas-fortress-economy/>

⁴¹ <https://www.uschina.org/reports/government-procurement-and-sales-state-owned-enterprises-china>; <https://www.prnewswire.com/news-releases/futurelogic-releases-china-tech-decoupled-report-providing-insights-on-chinas-xinchiang-industry-301433437.html>

⁴² <https://home.treasury.gov/news/press-releases/jy2455>

Securitization and China's Legal Regime

In addition to long-time trends of state involvement in China's political economy and amplified emphasis on indigenous innovation to boost the market shares of domestic firms in MiC2025 sectors dramatically at the expense of foreign competitors, the country's legal and security landscape under Xi Jinping has evolved in symbiosis with industrial policy objectives in ways that have substantially broadened the scope and rule-by-law basis for party-state intervention and, in turn, have eroded the commercial opportunities for foreign firms in the Chinese market. The PRC is not a rule-of-law system; a lack of an independent judiciary gives firms, domestic and global, little if any recourse to challenge state intervention when and if it occurs. Moreover, the lack of a free press and the general sensitivity of state legal actions make it impossible to know the timing, extent, and nature of state interventions under PRC law and when and how state media may be marshaled to undermine the reputation of foreign firms before the Chinese people in the PRC market.

In particular, firms should be aware of regulations and laws on national security, intelligence, cybersecurity, counter-espionage, data security, and more. The emphasis on security in contemporary China is unprecedented in the post-Mao era and affects basic firm activities like due diligence and economic research. Key laws include the following:

- **Counter-Espionage Law (2014, revised 2023):** The 2014 law stipulated that “citizens and organizations shall facilitate and provide other assistance to counter-espionage efforts” (Article 4), and the 2023 version expanded the government's role and the issue areas as well as requested additional public participation. Notably, the 2023 version expanded the scope of espionage activities to include “stealing, prying into, purchasing or illegally providing...other documents, data, materials, or items related to national security and interests” (Article 4). The law is to be enforced by the Ministry of State Security (MSS) and its local offices. The lack of clarity over “national security” and what “documents, data, materials, or items” might impinge on national security may leave much discretion for MSS personnel such that market research, due diligence, and data collection and dissemination on economic issues could be interpreted as national security relevant. In April 2023, **authorities raided** the offices of Bain, the Mintz Group, and more, detaining Chinese nationals, likely for conducting market research and investigations for clients. Advisory services such as these occupy a liminal space in China's system in the context of the Counter-Espionage Law, and the U.S. National Counterintelligence and Security Center **states** that the law's ambiguity can create “legal risks and uncertainty for foreign companies, journalists, academics, and researchers.”
- **National Security Law:** The **2015 National Security Law** establishes “economic security” and “financial stability” as pillars of national security (Articles 19, 20) and states that “enterprises and other organizations have the responsibility and obligation to preserve national security” (Article 11) and “shall cooperate as required by national security efforts” (Article 78). The U.S. National Counterintelligence and Security Center **has raised concerns** that the law “may compel locally employed PRC nationals of U.S. companies to assist in investigations that may expose operating elements of U.S. companies/persons.”

The **2020 Hong Kong National Security Law** extends a PRC security framework to Hong Kong, criminalizing “separatism, subversion, organization and perpetration of terrorist activities, and collusion with a foreign country or with external elements to endanger national security” (Article 1), when “secession” possibly includes speech acts that are interpreted as challenging the unity of Hong Kong and the PRC.

National Intelligence Law: The 2017 National Intelligence Law similarly requires that “all organizations and citizens shall support, assist, and cooperate with the state intelligence work” (Article 7). Again, the U.S. National Counterintelligence and Security Center **has expressed concerns** that the law “may force locally employed PRC nationals of U.S. companies to assist in PRC national intelligence efforts” and creates ‘affirmative’ legal responsibilities for PRC and foreign (including U.S.) entities” to do so.

- **Anti-Foreign Sanctions Law:** The 2021 Anti-Foreign Sanctions Law states that organizations or individuals may face countermeasures if they are involved with “discriminatory restrictive measures against Chinese citizens and organizations” (Article 4) and must not aid in implementing sanctions imposed by other countries (Article 12). The law may endanger companies perceived to aid in U.S. (or European Union or United Kingdom) sanctions, is ambiguous in what is meant by “assisting with foreign sanctions,” and may justify retaliatory measures against U.S. firms and/or create legal conflicts for companies operating in the United States and China.
- **Data and Cybersecurity Laws: The 2021 Data Security Law** outlines provisions on “data handling” and “data security” to “protect the lawful rights and interests of individuals and organizations, safeguard national sovereignty, security, and development interests” (Article 1) both within the PRC and internationally “[w]hen data handling activities outside the mainland territory of the PRC harm the national security, the public interest, or the lawful rights and interests of citizens and organizations of the PRC” (Article 2). Articles 31 and 32 require that outbound data are subject to the Cybersecurity law, and U.S. firms and foreign entities face uncertainty about regulatory requirements for cross-border data flows. The **2017 Cybersecurity Law** requires localization of data for “critical infrastructure” (Articles 31, 34) and empowers authorities to require “technical support and assistance to organs related to national security” (Article 28). The law targets “network operators,” and Article 76 indicates that “operators” includes organizations dealing with “network data” or “all kinds of electronic data collected, stored, transmitted, processed, and produced through networks.” Ultimately, the law applies to almost any entity dealing with digital data in China, and leaves “critical infrastructure” and “national security” undefined. Unlike the Counter-Espionage Law, the Data Security and Cybersecurity Laws are crafted and enforced by the Central Cyberspace Affairs Commission and the Cyberspace Administration of China, and overlapping and uncertain jurisdiction over data regulation **generates regulatory ambiguities** for U.S. firms.
- **Exit bans:** Many of these laws (e.g., Articles 33-35 of the Counter-Espionage Law) authorize entry and exit bans for “espionage” suspects regardless of nationality. Exit bans for personnel of U.S. businesses have risen in recent years. Although no systematic data exist for obvious reasons (media and government attention is not necessarily helpful), scholars have documented at least 100 cases.⁴³ These bans seem to typically target affiliates of firms with contract or judicial disputes in China, but the general opacity of the judicial system means sometimes executives do not know a dispute exists or that their firm is connected to a dispute between other parties. Other cases are deemed “commercial hostage taking.” Exit bans can apply when firms offend the Chinese government or are engaged in activities the PRC designates security relevant, such as sensitive data collection or due diligence, but publicly available data seem to indicate that most of the known exit ban cases (two-thirds) are in “standardized or commoditized” industries rather than in high-technology or immediately security-relevant sectors.⁴⁴

⁴³ Jack Wroldsen and Chris Carr. “The Rise of Exit Bans and Commercial Hostage Taking in China.” MIT Sloan Review. Vol. 65, Issue 1 (November 2023).

⁴⁴ Ibid.

- **Security agencies empowerment:** The general empowerment of China’s many state security organs, especially the MSS but including the Ministry of Commerce and the Ministry of Foreign Affairs, on economic and commercial matters presents significant risks for U.S. firms and their personnel in China beyond exit bans, including MSS visits to firm facilities or personnel short of detentions or raids and frequent invitations to tea, or informal summons for questioning, by MSS personnel. Grounds for such questioning could include anything from suspicions of violating one of these laws to general engagement with issues related to “national security,” an expanding set of activities.⁴⁵ In qualitative interviews, U.S. firms with China-based personnel expressed concerns and noted upticks in site visits from Chinese security personnel, especially from the MSS.⁴⁶ We learned that most firms are not always certain about the frequency of these visits or the reasons behind them. However, discussions with advisory service providers suggested that these visits are frequently coordinated and systematic. In addition to site visits, firms report that China-based personnel receive invitations for tea with local government, and sometimes central government, personnel. One company that supplies the U.S. federal government, including the Department of Defense (but does not manufacture products in China that are supplied to the U.S. government), reported consistent tea invitations and perceived pressure to both convey information about how the U.S. government protects information security and also to “choose supplying Chinese firms over supplying the U.S. government.” Most companies answered questions about tea invitations with expressions of concern that they are certain it happens but do not know when and why and do not have clear means of eliciting and acting on this information. Firms with connections, even indirect, to new outbound restrictions note an increase in tea invitations and MSS visits or rumors of such in their networks. One interviewee stated that Chinese government officials appear eager for information from firms on which sectors are likely next to face such restrictions.

- **Export controls:** China has moved in recent years to establish legal groundwork for export controls. In summer 2023, China moved to prohibit the export of gallium and germanium, both critical inputs in high-technology supply chains.⁴⁷ The Export Control Law was first promulgated in 2020, and **new rules in 2024** seemed to mirror U.S. rules about “de minimis” and the Foreign Direct Product Rule (see Section III). In 2024, the China Central Military Commission was **listed as co-issuer of export controls**, elevating the role of security ministries in commercial matters.

- **Extraterritoriality:** Increasingly, China has sought extraterritorial application of these and other laws, strengthening rules under the Anti-Monopoly Law, Anti-Foreign Sanctions Law, Cybersecurity Law, and more to apply to businesses with significant market presence in China. The extraterritorial extension gives companies few easy choices as they navigate compliance with U.S. sanctions and restrictions and China’s countermeasures, and it expands uncertainty and the leverage of the PRC government.

⁴⁵ <https://www.scmp.com/news/china/politics/article/3250419/10-cups-tea-first-time-chinas-top-intelligence-agency-spells-out-reasons-questioning-authorities>

⁴⁶ <https://www.prcleader.org/post/piercing-the-veil-of-secrecy-the-surveillance-role-of-china-s-mss-and-mps>

⁴⁷ https://www.usitc.gov/publications/332/executive_briefings/ebot_germanium_and_gallium.pdf

Political “red lines” and the potential for reprisal for firm and firm personnel have become prominent under Xi Jinping in ways that pose some risks for U.S. firms. Many of these “red lines” concern the statuses of Tibet, Hong Kong, or Xinjiang and are not new to China’s political environment, but, under Xi Jinping and with growing controversy and external scrutiny of the PRC’s actions in those areas, politicization of corporate and individual statements has become routine. These requirements are tied to the legal regime, as many statements about the status of Hong Kong, Taiwan, Tibet, and more have become criminalized as a result of laws that govern national security. Many international firms have been pressured to issue apologies when their statements or marketing materials ran afoul of PRC politics, for example, listing Taiwan or Hong Kong as countries or separate from China on websites or maps, quoting figures the PRC considers dissidents, or when personnel have expressed support for political movements (e.g., in Hong Kong) that China considers dangerous.⁴⁸

A Synthetic Problem

We note that these laws weave together in a way that creates ambiguity and tensions for firms and persistent leverage for the PRC government. Firms are limited in the concerns they can voice and are constrained by laws that give the government broad remit to apply punitive sanctions. The threat of exit bans further impedes companies from reporting what challenges they face or what interventions they have experienced. Moreover, the breadth of government actors and actions leaves firms uncertain about the level of coordination among government agencies, such that different parts of firms may address threats and interactions separately, and companies may therefore lack a whole-of-firm view.

⁴⁸ For example, Apple hosted a map app used by Hong Kong protestors to track police movements in 2019; Tiffany & Co. used an ad with model Sun Feigei covering one eye in what was interpreted as a reference to protests in Hong Kong in 2019; McDonald’s in 2019 aired a TV ad in Taiwan showing a student with an ID and Taiwan listed as a country; Marriott listed Taiwan, Tibet, and Hong Kong as countries on a customer survey in 2019; and Intel in 2021 instructed suppliers not to procure from Xinjiang. All these corporations were pressured to issue apologies to China. See Margaret M. Pearson, Meg Rithmire, and Kellee S. Tsai. 2022. “China’s Party-State Capitalism and International Backlash: From Interdependence to Insecurity.” *International Security*, 47(2): 156–7.

Annex II: U.S. Legal and Regulatory Landscape

I. Federal Regulatory and Legislative Landscape

The United States' whole-of-government approach to national security risks from China continues to expand through executive and congressional action. In 2024 and early January 2025 alone:

- The Commerce Department's Bureau of Industry and Security (BIS) issued controls aimed at, among other things, restricting China's ability to obtain advanced computing chips, develop and maintain supercomputers, and manufacture advanced semiconductors.
- In October 2024, the Department of the Treasury, as chair of CFIUS, issued a final rule modifying and expanding CFIUS's jurisdiction over certain real estate transactions involving foreign persons by adding over 50 military installations, across 30 states, to the existing list of installations around which CFIUS currently has jurisdiction.⁴⁹ On November 26, 2024, Treasury also published its final rule that expanded CFIUS's authorities to inquire into transactions not formally notified to it, thus enhancing its penalty authorities for failure to file timely mandatory notices or breaches of mitigation agreements with CFIUS.⁵⁰
- On October 28, 2024, Treasury published its long-awaited final regulations (the Outbound Rule) to implement the Outbound Order issued by President Biden on August 9, 2023.⁵¹ The Outbound Rule notes that Treasury is focused on restricting the transfer of "intangible benefits" that may be exploited by foreign entities of concern to the detriment of U.S. national security. The final regulations went into effect on January 2, 2025.⁵²
- On December 27, 2024, the U.S. Department of Justice (DOJ) issued the Final Rule implementing President Biden's February 28, 2024, Executive Order on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (Bulk Personal Data EO).
- On January 3, 2025, the Commerce Department issued an advance notice of proposed rulemaking (ANPRM) to address risks associated with ICTS in unmanned aircraft systems (UASs) or drones. The ANPRM aims to secure the drone ICTS supply chain and protect U.S. national security from potential threats posed by foreign adversaries, particularly China and Russia.

⁴⁹ <https://home.treasury.gov/news/press-releases/jy2708>

⁵⁰ 89 Fed. Reg. 93179 et seq. (November 26, 2024).

⁵¹ Executive Order 14105, "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern" (August 9, 2023).

⁵² <https://www.federalregister.gov/documents/2024/11/15/2024-25422/provisions-pertaining-to-us-investments-in-certain-national-security-technologies-and-products-in>

- From January 14, 2025, BIS, through its Office of Information and Communication Technology and Services (ICTS), released its final rule (Connected Vehicle Final Rule) to address national security risks posed by connected vehicles (CVs) from countries of concern.
- From January 15 to 16, 2025, BIS issued three interim final rules focusing on tighter controls related to artificial intelligence and other advanced technologies: (1) a “Framework for Artificial Intelligence Diffusion,” which applied new controls on advanced computing integrated circuits (ICs) and model weights for certain advanced closed-weight dual-use AI models; (2) further revisions and enhancements to controls for access to advanced ICs, particularly focused on due diligence procedures for foundries and Outsourced Assembly and Test (OSAT) companies; and (3) new license requirements for certain advanced biotechnology systems and equipment which can “facilitate the development of AI and biological design tools.”

Expansions of Existing Authorities

1. CFIUS

Since the enactment of the Foreign Investment Risk Review Modernization Act in 2018, CFIUS has seen a steady increase in overall activity, backed by dramatic increases in staff and expanded funding. CFIUS continues to experience a heavy caseload, formally reviewing 233 notices in 2023 and monitoring a record 246 mitigation agreements, 36 of which were entered into for transactions filed in 2023, based on its most recent annual **report** (2023 Report). The committee issued four civil monetary penalties of unspecified amounts for violations of mitigation agreements and noted in its 2023 Report that this is twice the number of penalties issued during CFIUS’s nearly 50-year history. The 2023 Report also states that the committee evaluated “thousands” of potential nonnotified transactions.

Most recently, on November 1, 2024, Treasury **issued** a final rule to modify and expand CFIUS’s jurisdiction over the acquisition of certain real estate in the United States by foreign persons by adding over 50 military installations, across 30 states, to the existing list of installations around which CFIUS currently has jurisdiction. This proposed expansion likely stems from mounting concerns—from the public, Congress, and the Biden administration—regarding foreign land acquisitions near U.S. military installations, as signaled by President Biden’s May 13, 2024, divestiture order related to an acquisition by Chinese national-owned MineOne Partners Ltd. This was the first Presidential order arising out of CFIUS that relied on the real estate provisions of the CFIUS regulations to prohibit an acquisition of real estate within the United States.

2. Export Controls

The Biden administration also sought to address national security concerns stemming from China’s access to certain sensitive technologies through export controls. On March 29, 2024, the U.S. Commerce Department’s BIS announced an interim final rule that introduces new controls in the Export Administration Regulations (EAR) aimed at restricting China’s ability to obtain advanced computing chips, develop and maintain supercomputers, and manufacture advanced semiconductors. These new controls were first introduced on October 7, 2022, and expanded on October 17, 2023. They add certain advanced chips, computer commodities containing such chips, and certain semiconductor manufacturing equipment to the Commerce Control List of the EAR and notably expand EAR’s scope to reach additional items produced outside the United States.

They also restrict the ability of U.S. persons to support the development or production of integrated circuits at certain semiconductor fabrication facilities in China and add new license requirements for certain items destined to China, including certain items for use in supercomputers and the development or production of semiconductors or semiconductor manufacturing equipment that meet certain technical parameters. On July 25, 2024, BIS issued additional proposed rules that would impose enhanced restrictions on exports, reexports, and in-country transfers of items subject to the EAR and U.S. person support for foreign military, intelligence, and security services. Among other issues, the proposed rules focus on expanding end use and end user controls to apply to all items subject to the EAR when destined to the armed forces, national guard, or paramilitary forces of countries subject to a U.S. arms embargo (such as China). On December 2, 2024, BIS issued an interim final rule further revising and expanding the controls in the EAR on advanced computing and semiconductor manufacturing, along with a final rule that designated an additional 140 entities to its Entity List, placing export restrictions and licensing requirements for certain technologies and goods.

Further, on January 15, 2025, BIS issued several interim final rules revising the EAR to enhance controls related to certain advanced technologies. First, BIS issued the Framework for AI Diffusion rule, which, as BIS summarized, seeks to add “controls on advanced computing integrated circuits (ICs) and adds a new control on artificial intelligence (AI) model weights for certain advanced closed-weight dual-use AI models.”⁵³

Second, BIS published revisions to controls governing access to advanced ICs. Specifically, the revised rules focus “on providing ‘front-end fabricators’ with objective, bright-line rules designed to assist in better identifying transactions with potential risk for diversion in a manner contrary to U.S. national security and foreign policy interests; enhancing due diligence procedures to ensure that new customers are appropriately vetted by ‘front-end fabricators’ prior to providing ICs that may meet the advanced computing control levels; and improving reporting for transactions involving newer customers who may pose a heightened risk of diversion.”⁵⁴

Third, BIS published an interim final rule revising the EAR to impose new controls on certain biotechnology equipment and related technology. BIS stated the new controls are necessary to protect U.S. national security and foreign policy interests “given the dual-use nature and relevance of specific biotechnology equipment to contribute to the research and development of certain militarily relevant technologies.”⁵⁵ The rule further indicates that biotechnology, “particularly when coupled with AI and biological design tools,” could strengthen the military capabilities of countries of concern, and that the U.S. government’s concerns relate to the potential “combination of biotechnology with other enabling technologies for asymmetric military advantage.”

3. Regulations Related to Securing the ICTS Supply Chain

On June 16, 2023, the Commerce Department published its Final Rule on Securing the ICTS Supply Chain (the ICTS Final Rule) to implement provisions of EO, “Protecting Americans’ Sensitive Data from Foreign Adversaries,” issued by President Biden on June 9, 2021 (EO 14034). The Final Rule retained the core elements of the Notice of Published Rulemaking (ICTS NPRM) released on November 26, 2021, which proposed amendments to Commerce Department’s Interim Final Rule on ICTS that was published on January 19, 2021 (the Interim Rule).

⁵³ <https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion>

⁵⁴ <https://www.federalregister.gov/documents/2025/01/16/2025-00711/implementation-of-additional-due-diligence-measures-for-advanced-computing-integrated-circuits>

⁵⁵ <https://www.federalregister.gov/documents/2025/01/16/2025-00723/controls-on-certain-laboratory-equipment-and-related-technology-to-address-dual-use-concerns-about>

The Interim Rule had implemented EO 13873, “Securing the ICTS Supply Chain” issued by President Trump on May 15, 2019 (ICTS EO). The ICTS Final Rule is broad in scope, defining an “ICTS transaction” as “any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download.” To be a transaction that would be subject to the Commerce Department’s review, the transaction must meet the following criteria:

- Is conducted by any person subject to the jurisdiction of the United States or involves property subject to the jurisdiction of the United States
- Involves any property in which any foreign country or a national thereof has an interest (including through an interest in a contract for the provision of the technology or service)
- Is initiated, pending, or completed on or after January 19, 2021
- Involves one of the ICTS listed in **Section 7.3(4)** of the ICTS Rule

On June 24, 2024, the Commerce Department issued its first-ever final determination and prohibition pursuant to the ICTS EO when it prohibited Kaspersky Lab, Inc., its affiliates, subsidiaries, and parent companies (Kaspersky) from directly or indirectly providing antivirus software and cybersecurity products or services in the United States or to U.S. persons. The **determination** concluded, after a years-long investigation by the Commerce Department, that Kaspersky’s continued operations in the United States—and specifically, Kaspersky’s provision of cybersecurity and antivirus software to U.S. persons, including through third-party entities that integrate Kaspersky cybersecurity or antivirus software into commercial hardware or software—pose undue and unacceptable risks to U.S. national security and to the security and safety of U.S. persons that could not be addressed through mitigation measures short of a total prohibition. The implementation of the ICTS Final Rule and the Commerce Department’s first-ever prohibition signal that the Commerce Department’s authorities under the ICTS EO could become an additional tool in the U.S. government’s growing national security toolkit to address risks from countries of concern.

i. Regulations Related to Connected Vehicles

The Biden administration expanded its regulatory arsenal specifically to address risks posed by Chinese CV technology and has directed the Department of Commerce to “investigate the national security risks from CVs that incorporate technology from countries of concern, including China.” Then-Commerce Secretary Gina Raimondo **indicated** publicly that the U.S. government could take “extreme action” and ban Chinese CVs in the United States. The rules issued by the Commerce Department go further than Chinese-owned CV companies and would encompass certain other technologies and software developed in China regardless of the nationality of the companies developing them—an approach that is much more akin to “decoupling” than to “de-risking.” Specifically, on January 14, 2025, the Commerce Department’s BIS published the **Connected Vehicle Final Rule** that would prohibit the import of certain hardware related to Vehicle Connectivity Systems (VCSs) from the PRC and Russia. The Connected Vehicle Final Rule further prohibits the sale or import of CVs that incorporate certain software related to VCSs or automated driving systems. Parties who import nonprohibited VCS hardware or import or sell vehicles that incorporate nonprohibited covered software will be required to submit “declarations of conformity” to BIS covering all relevant VCS hardware and each group of relevant model year vehicles to confirm that such VCS hardware is not prohibited or that such vehicles do not incorporate

prohibited covered software, as applicable. The Connected Vehicle Final Rule also provides general authorizations to allow certain parties to undertake otherwise prohibited transactions to “minimize unanticipated and unnecessary disruption to industry.” Additionally, the Connected Vehicle Final Rule indicates that the Commerce Department will consider specific authorizations, which, after an application to and approval by BIS, grant VCS hardware importers and CV manufacturers the ability to engage in otherwise prohibited transactions, including because the associated undue or unacceptable risks have been, or can be, mitigated.

The Biden administration’s focus on CV technology mirrored similar bipartisan sentiment in the U.S. Congress. On April 18, 2024, Ranking Member Raja Krishnamoorthi and Chairman Mike Gallagher of the China Select Committee **sent** a letter to Defense Secretary Lloyd Austin urging the Pentagon to ban CVs containing Chinese-produced technologies from entering U.S. military bases. The China Select Committee **issued** another letter in November 2023, calling for an investigation into all Chinese Light Detection and Ranging (LiDAR) companies that could pose data security and national security risks. That letter came only weeks after a bipartisan group of U.S. lawmakers **asked** 10 Chinese companies to share information about their data collection and testing practices in the United States.

New Regulations

1. Regulations Related to Outbound Investment Screening

As noted, the Biden administration on August 9, 2023, released the Outbound Order proposing (1) prohibitions on certain outbound investments in the semiconductors and microelectronics, quantum information technologies, and artificial intelligence (AI) sectors (the Identified Sectors) and (2) mandatory notification requirements for a broader set of transactions in those same sectors, in each case focused on China. The Outbound Order marks the first time that the United States, or any other major Western democratic economy, has sought to regulate and control outbound capital flows and other investments for national security reasons. The requirements would apply to U.S. investments in Chinese companies, including Chinese majority-owned subsidiaries outside of China, engaged in certain activities related to the Identified Sectors. More generally, Treasury’s final rule on outbound investment, which went into effect on January 2, 2025, sets forth regulations that would cause the notification requirements and prohibitions to apply broadly to transactions not only in China, but globally—including in the United States—where the transaction parties are U.S. and Chinese, or ultimately U.S. and Chinese owned—in particular across much of the global semiconductor industry.

In parallel with the development of executive branch regulation, Congress has made continuing efforts to legislate restrictions on outbound investment, potentially by expanding on the EO by including additional covered sectors and taking a notification-only approach.

2. Regulations Related to the Protection of U.S. Sensitive Personal Data

On February 28, 2024, President Biden signed the “Bulk Personal Data EO,” representing the first time the U.S. government has sought to regulate U.S. personal data for national security reasons—as opposed to privacy or other reasons. On December 27, 2024, DOJ issued its final regulations (Personal Data Final Rule) implementing the Bulk Personal Data EO. The final regulations detail the substance of contemplated implementing regulations for the EO and would establish an entirely new regulatory regime, led by DOJ and involving other U.S. government agencies, including the Department of Homeland Security. The Personal Data Final Rule contemplates not only flat prohibitions on certain transfers of bulk personal data but also a range of requirements that would apply to companies that engage in certain categories of investment, vendor, and employment transactions—essentially making those companies regulated entities for national security purposes. The final regulations also establish bright line rules to prevent access to certain sensitive personal data of U.S. persons by “countries of concern”—including China and Russia—and thereby mitigate the risk that such data could be exploited or used in ways that would harm U.S. national security.

The Personal Data EO was motivated by concerns about U.S. national security risks arising from foreign access to personal data and a perception that existing U.S. law is not sufficient to address those concerns. As explained in the Personal Data EO and NPRM, the Biden administration determined that “certain countries of concern” are using U.S. sensitive personal data to engage in a wide range of malicious activities that harm U.S. national security interests, including by using it for purposes of espionage, influence, kinetic or cyber operations, and to identify other strategic advantages over the United States. Over the past decade, issues related to personal data have featured prominently in numerous transactions reviewed by CFIUS and the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (better known as “Team Telecom”), including many transactions that were prohibited on national security grounds. In other cases, CFIUS and Team Telecom have required as a condition of approval that parties enter into “mitigation agreements” focused on the protection of personal data. The Personal Data EO addresses these risks more holistically rather than in individual M&A transactions or investments.

Specifically, the Personal Data Final Rule contemplates a regime that would prohibit or otherwise restrict U.S. persons from engaging in “covered data transactions,” which are certain transactions that involve the transfer of bulk “U.S. sensitive personal data” or “U.S. Government-related data” to “countries of concern.” The regime will not involve a case-by-case analysis or adjudication of transactions but instead will impose outright prohibitions on certain transactions and will presumptively prohibit certain other classes of transactions, unless the transaction parties adopt security practices issued by the Cybersecurity and Infrastructure Security Agency on January 3, 2025, under the Department of Homeland Security. Parties may seek licenses to engage in transactions that otherwise would be prohibited or restricted (though only in “rare circumstances”), as well as advisory opinions with respect to the application of the rules. The final regulations also require that U.S. persons engaged in any transaction subject to the regulations prepare and maintain records of each such transaction for at least 10 years after the date of the transaction.

On April 24, 2024, President Biden signed into law H.R. 815, which includes the Protecting Americans' Data from Foreign Adversaries Act of 2024, a bill that passed the House 414-0 as H.R. 7520 on March 20. The Act is one of several recent actions by the U.S. government to regulate transfers of U.S. personal data for national security reasons, reflecting heightened concerns about access to sensitive personal data by “foreign adversaries,” with a particular focus on China. Although the policy objectives are similar, the law takes a different approach compared to the Personal Data EO. The Act makes it unlawful for data brokers to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a U.S. individual (i.e., people residing in the United States) to any foreign adversary or any entity controlled by a foreign adversary.

3. Regulations Related to Unmanned Aerial Vehicles

On January 2, 2025, the Commerce Department's BIS **issued** an advance notice of proposed rulemaking to address risks associated with information and communications technology and services in UASs or drones (Drone ANPRM). The Drone ANPRM proposes a broad approach, targeting not only unmanned aerial vehicles but also ground control stations, communication links, and other associated components and would regulate various actors across the UAS supply chain, including UAS companies, original equipment manufacturers, and service providers to address potential threats posed by foreign adversaries, particularly China and Russia.

4. IaaS Rule

In connection with EO 14110 signed by President Biden in October 2023 regarding the “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,” the Commerce Department was directed to issue regulations requiring that U.S. infrastructure-as-a-service (IaaS) providers report to the Commerce Department when a foreign person transacts with such a provider to train certain large AI models. The **relevant Notice of Proposed Rulemaking (IaaS NPRM)** was issued on January 29, 2024, and contemplates many know-your-customer requirements pertaining to the use of U.S. IaaS products and services, as well as the reporting requirements related to the use of U.S. IaaS products or services to train certain AI models. The clear purpose of the proposed regulations is to limit the use of U.S.-based cloud infrastructure by Chinese parties in connection with their efforts to train certain AI models.

Other Legislative Actions

In addition to the areas identified, the U.S. Congress has been, and is likely to remain, actively focused on legislation that would provide regulation of China-related risks on national security grounds. Enhanced export controls,⁵⁶ greater regulation in the biotechnology area,⁵⁷ and even further CFIUS reform are all areas of potential additional legislation.

II. State Regulatory and Legislative Landscape

Mirroring the mood in Washington, state governments in the United States have taken an expansive approach to regulation of potential national security risks from China, with a focus on following areas: (1) foreign acquisition of U.S. agricultural lands or other real estate located near critical infrastructure; (2) contracts between state government bodies and foreign entities; and (3) investments by state government funds into foreign entities, among other areas.

Real Estate Transactions

A recurring area of activity for state governments has been Chinese acquisition of U.S. real estate. As of April 25, 2024, various states have signed 31 bills into law that restrict property ownership by Chinese entities.⁵⁸ From January 1 to April 25, 2024, 78 bills restricting property ownership were proposed and were under active consideration by state legislatures. In addition to regulating the sale of agricultural land, several states have also banned Chinese companies or nonresident Chinese individuals from purchasing property located within a certain radius of a military installation or critical infrastructure facility. States have adopted various definitions for critical infrastructure facilities. Florida's Senate Bill 264, for example, includes any of the following as critical infrastructure: a chemical manufacturing facility, a refinery, an electrical power plant, a water treatment facility or wastewater treatment plant, a liquid natural gas terminal, a telecommunications central switching office, a gas processing plant, a seaport, a spaceport territory, or an airport.⁵⁹ Oklahoma's law (Senate Bill 1705) even more broadly bans aliens, noncitizens, and foreign government adversaries from "acquir[ing] title or own[ing] land" in the state subject to a few exceptions.⁶⁰

States have also adopted various definitions for covered entities that would be prohibited from purchasing land. On the narrower end, Idaho's House Bill 496, signed into law in March 2024, bans a "foreign government or a foreign state-controlled enterprise."⁶¹ On the broader end, Georgia's Senate Bill 420, signed into law in April 2024, bans all "nonresident aliens."⁶² On October 17, 2023, the Arkansas Attorney General ordered a subsidiary of a company that was ultimately owned by the China National Chemical Company to divest from 160 acres of farmland.⁶³

⁵⁶ See, for example, <https://www.congress.gov/bill/118th-congress/house-bill/8315>.

⁵⁷ See, for example, <https://www.congress.gov/bill/118th-congress/senate-bill/3558/text>.

⁵⁸ Committee of 100, "Federal and State Bills Restricting Property Ownership by Foreign Entities," last visited on July 11, 2024, <https://www.committee100.org/our-work/federal-and-state-bills-prohibiting-property-ownership-by-foreign-individuals-and-entities/>.

⁵⁹ Florida Senate Bill 264 Sec. 692.201, signed into law on May 9, 2023, <https://legiscan.com/FL/text/S0264/2023>.

⁶⁰ Oklahoma Senate Bill 1705 Sec. 121, signed into law on May 31, 2024, <https://legiscan.com/OK/bill/SB1705/2024>.

⁶¹ Idaho House Bill 496 Sec. 55-103, signed into law on March 12, 2024, <https://legiscan.com/ID/bill/H0496/2024>.

⁶² Georgia Senate Bill 420 Sec. 2-1-7, signed into law on April 30, 2024, <https://legiscan.com/GA/text/SB420/id/2906549>.

⁶³ Tim Griffin, Letter Concerning Northrup King Seed Co., October 17, 2023, <https://arkansasag.gov/wp-content/uploads/2023-10-17-Syngenta-ChemChina-Enforcement-Letter.pdf>.

Restrictions on State Government Contracts and Devices

States have also passed legislation restricting state agencies from contracting with certain Chinese parties. Georgia's Senate Bill 346, signed into law on May 4, 2022, states that any company owned or operated by the government of China "shall be ineligible to, and shall not, bid on or submit a proposal for a contract with a state agency for goods or services."⁶⁴ Idaho's House Bill 294, which was signed into law on April 6, 2023, is similarly broad, banning government agencies from contracting with a company to "acquire or dispose of services, supplies, information technology, or construction" if that company is currently owned or operated by the government of China.⁶⁵

Other states have passed more targeted bans for contracts involving critical infrastructure, such as Indiana's Senate Bill 477, which was signed into law on May 1, 2023, or Louisiana's Senate Bill 472, which was signed into law on June 18, 2022.⁶⁶ A growing number of states have also passed and proposed legislation that would ban state government bodies from contracting with Chinese companies to purchase drones. Arkansas House Bill 1653 (2023) serves as an example: "A public entity shall not purchase a small, unmanned aircraft system that is manufactured or assembled by a covered foreign entity."⁶⁷

Public Funds and Divestment

Several state governments have sought to identify and mitigate against risks from public investments in Chinese companies. For instance, Florida and Indiana have officially passed laws that prohibit state funds from acquiring new investments in Chinese companies and that require state funds to divest any money currently invested in such companies.⁶⁸ Missouri's State Employees Retirement Fund also voted in December 2023 to divest its holdings in Chinese-owned companies.⁶⁹ Other states have proposed legislation that would adopt similar measures, including certain proposals that would prohibit state-managed funds from depositing money in banks located within China.⁷⁰ Even outside the context of formal legislation, certain states have communicated to private U.S. companies an interest in developing opportunities to divest from China. On May 16, 2023, the governors for South Dakota, Iowa, Mississippi, and Texas sent a letter to the CEO of Vanguard encouraging Vanguard to create a new emerging markets fund that excludes any investments in China.⁷¹ Such developments mirror a broader effort at the federal level to scrutinize outbound investments into China.

⁶⁴ Georgia Senate Bill 364 Sec. 50-5-84.1, signed into law on May 4, 2022, <https://legiscan.com/GA/text/SB346/2021>.

⁶⁵ Idaho House Bill 294 Sec. 67-2359, signed into law on April 3, 2023, <https://legiscan.com/ID/bill/H0294/2023>.

⁶⁶ Indiana Senate Bill 477 Sec. 1-1-16, signed into law on May 1, 2023, <https://legiscan.com/IN/bill/SB0477/2023>; Louisiana Senate Bill 472 Sec. 3051, signed into law on June 18, 2022, <https://legiscan.com/LA/text/SB472/2022>.

⁶⁷ Arkansas House Bill 1653 Sec. 25-1-127, signed into law on April 10, 2023, <https://legiscan.com/AR/text/HB1653/2023>.

⁶⁸ Florida House Bill 7071 Sec. 215.4735, signed into law on May 16, 2024, <https://legiscan.com/FL/text/H7071/2024>; Indiana Senate Bill 268 Sec. 5-10.2-13, signed into law on May 1, 2023, <https://legiscan.com/IN/bill/SB0268/2023>.

⁶⁹ Rudi Keller. December 12, 2023. "State Board Votes to Divest Missouri Employee Pension Fund from China." Missouri Independent. <https://missouriindependent.com/2023/12/12/state-board-votes-to-divest-missouri-pension-fund-from-china/#:~:text=The%20board%20overseeing%20Missouri's%20largest,decision%20it%20made%20last%20month>.

⁷⁰ See, for example, Alaska House Bill 94, introduced on March 6, 2023, <https://legiscan.com/AK/bill/HB94/2023>; Illinois House Bill 2984 Sec. 22.10, introduced September 8, 2023, <https://legiscan.com/IL/comments/HB2984/2023>; New Jersey Senate Bill 1365, introduced January 9, 2024, <https://legiscan.com/NJ/text/S1365/id/2876453>; Pennsylvania Senate Bill 1141, introduced on April 5, 2024, <https://legiscan.com/PA/bill/SB1141/2023>.

⁷¹ Kristi Noem et al. May 16, 2023. Letter to Mortimer Buckley. https://governor.sd.gov/doc/Joint-GovernorLetter-to-Vanguard-on-China_5-16-23.pdf.

III. Reputational Considerations

As noted, the pervasive mood in the U.S. government is that existing regulatory and legal frameworks have not caught up to the evolving geopolitical contours of U.S.-China competition and are not sufficient to address U.S. national security concerns. As a result, business in China and with Chinese parties has come under unprecedented scrutiny, and the scope of business sectors and relationships seen as presenting national security risks has also expanded. U.S. regulators, such as CFIUS, now routinely explore both foreign investors and U.S. parties' relationships in China as well as their internal policies and documents related to business in China. In other words, business relationships that are viewed as potentially advancing Chinese interests—even if in full compliance with U.S. law—have become more likely to create reputational risk.

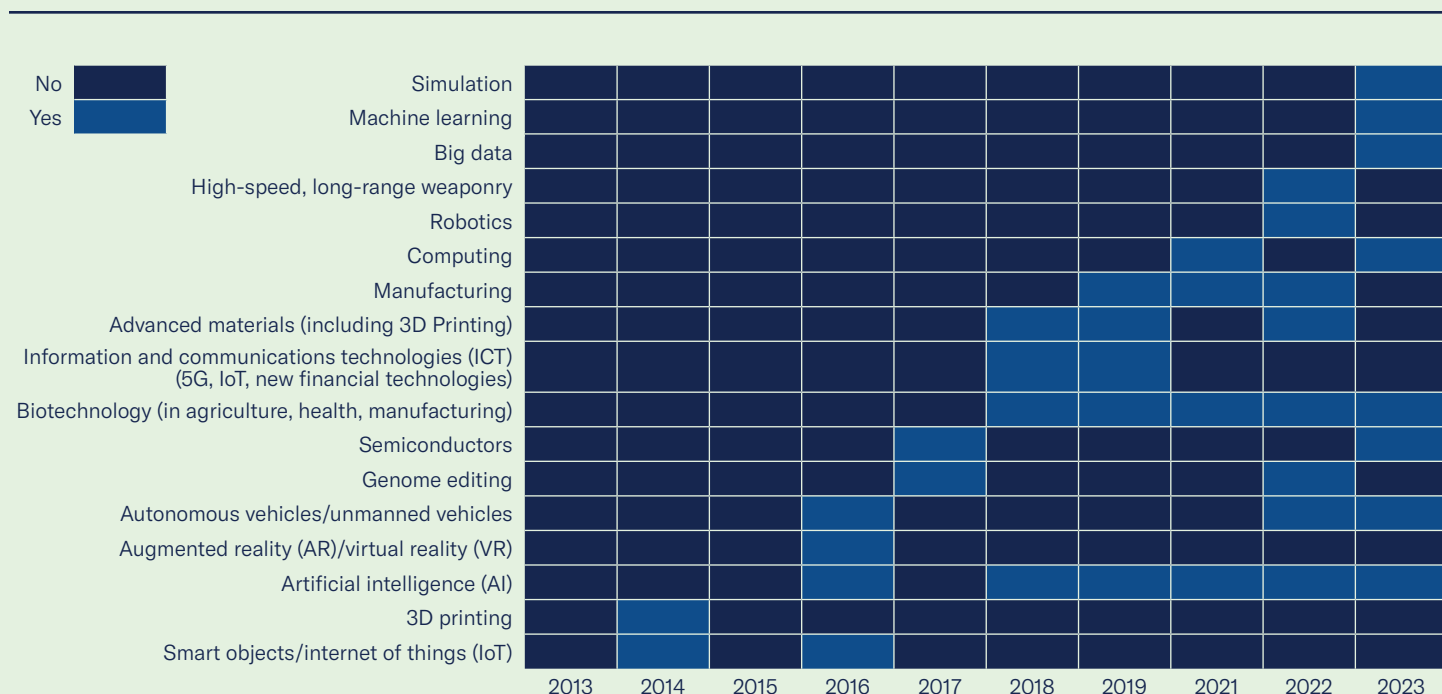
In this context, relationships with Chinese parties could manifest as a reputational matter on multiple fronts, including not only via Congress (e.g., investigations by the House China Select Committee) and regulatory processes such as CFIUS, but also third-party reports (including media reporting) and other forums where a company may have an interest, such as funding from the Commerce Department and even from a company's own U.S. customers, whose requirements related to China increasingly mirror the U.S. government's posture. For instance, in March 2023, the *Wall Street Journal* **reported** on the national security risks of Chinese state-owned cranes, which ultimately led to two U.S. Congressional committees **deciding** to investigate Swiss engineering group ABB's operations and ties to state-owned Shanghai Zhenhua Heavy Industries Company in China. The increasing potential for public scrutiny means that any business relationships in China should be evaluated not only from a legal compliance standpoint but also as a serious reputational risk matter in the context of an intensifying geopolitical rivalry with China.

Annex III: National Security and Risk

As both the United States and China have emerged as technologically advanced economies, and as competition has deepened in a broader range of sectors, the scope of national security concerns has expanded, and the lines between national security and economic security have blurred, if not disappeared entirely. Supply chains for many technological goods and services traverse dozens of national borders. A 2021 White House supply chain review report sought to understand the global complexity in supply chains for what it called “critical sectors” (semiconductors, batteries, critical minerals, pharmaceuticals, and defense). The reports detailed extensive Chinese involvement, and sometimes dominance, in these sectors, sometimes at such deep points in the supply chain or markets for raw materials that companies are unaware of their implicit dependence on Chinese supplies.⁷²

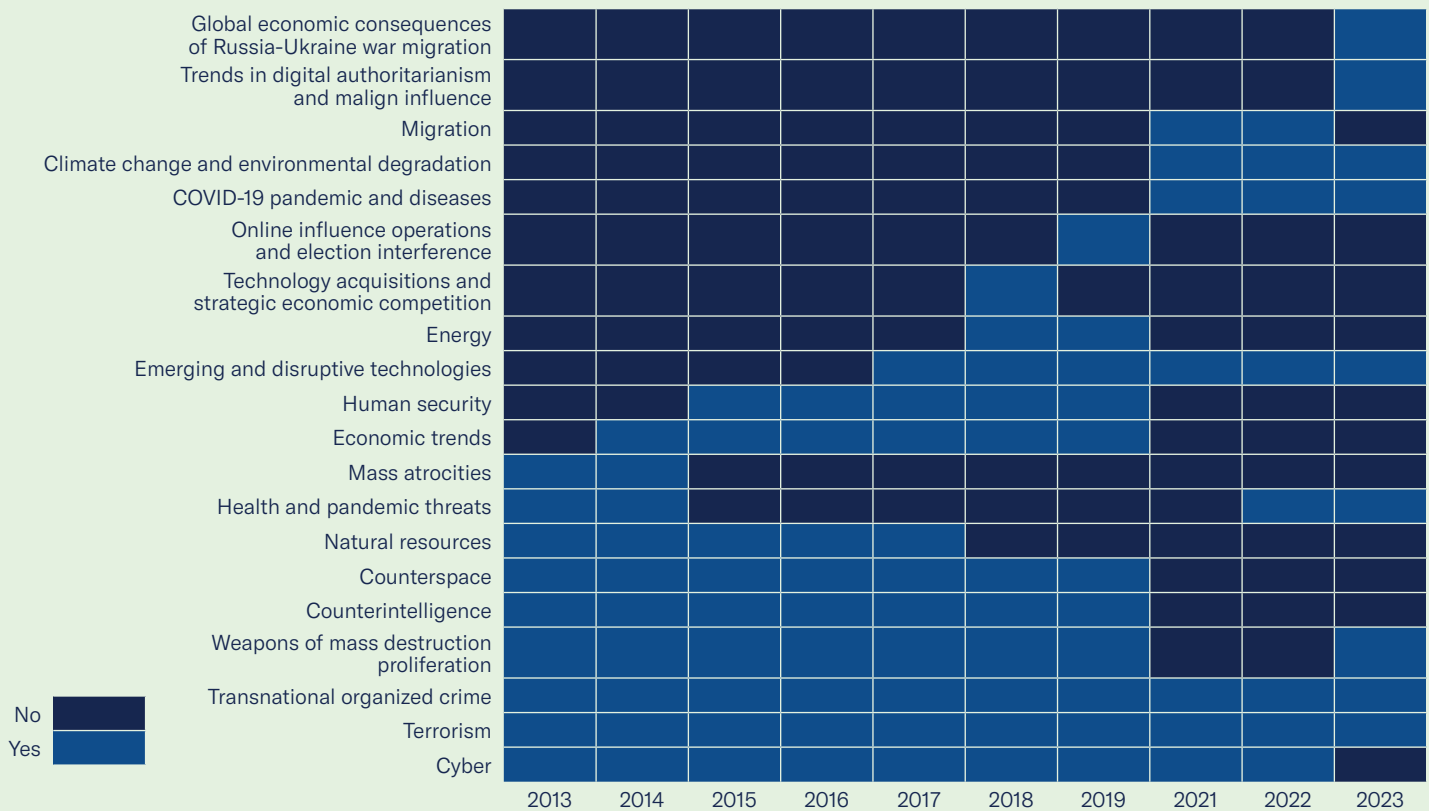
Definitions of “national security” as it relates to economic interdependence have been unstable, with a trend toward expanding what sectors and products are included in consideration of national security. Figures A3.1a and A3.1b visualize what technologies receive mention in the U.S. Director of National Intelligence Annual Threat Assessments from 2013 to 2023. The clear trend is an expanding and unstable set of technologies with national security threat relevance. As a result, even companies that do not directly produce in security-critical products or services are more likely to rely on such technologies in their own production processes.

Figure A3.1a



⁷² <https://www.bis.doc.gov/index.php/documents/technology-evaluation/2958-100-day-supply-chain-review-report>

Figure A3.1b

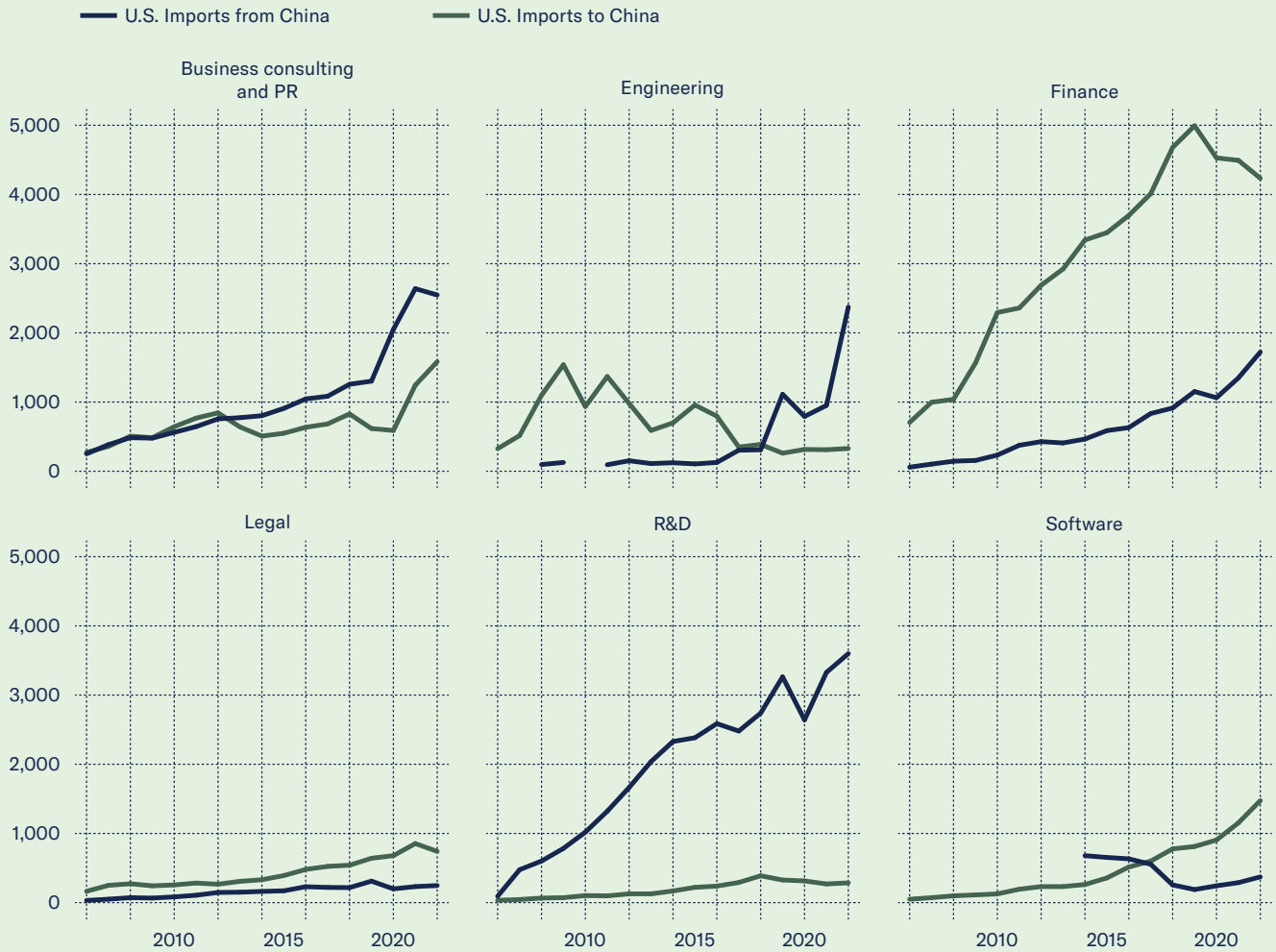


Because the landscape has shifted rapidly, firms and their products, services, networks, and activities are at the center of national efforts to protect national and “economic” security and changing definitions of what constitutes security. At the same time, firms are engaged in digital transformations, as business in any sector becomes more data-driven and data-intensive and new sectors emerge with technological advancement. This advancement is driven, in many cases, by precisely the kinds of cross-border collaboration and competition that is now viewed as a source of vulnerability for national interests.

For a subset of technologies, especially emerging sectors like artificial intelligence or quantum computing, Chinese advancement is viewed by the U.S. national security community as a particularly acute threat to the United States. This logic motivated the Biden administration’s Executive Order on outbound investment controls, with National Security advisor Jake Sullivan stating: “[W]e must usher in a third wave of the digital revolution—to ensure that emerging technologies work for, and not against, our democracies and security,” and “[g]iven the foundational nature of certain technologies, such as advanced logic and memory chips, we must maintain as large a lead as possible [over adversaries].”⁷³ Some in Washington have asserted an even more aggressive position, arguing that anything that advances China’s “comprehensive national power”—whether involved in emerging sectors or not—is a threat to the United States. These broader concerns are especially relevant for U.S. companies providing financial, legal, or advisory services to the Chinese market, which is a substantial part of the bilateral business relationship. Although the United States has long experienced a trade deficit with China in goods, the balance of trade in services is in surplus in many categories, except for engineering and research and development (see Figure A3.2).

⁷³ <https://bostonglobalforum.org/news/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/>

Figure A3.2



For such adjacent sectors, or less technologically advanced sectors, many policymakers worry about national security risks without adequately examining the tradeoffs and costs to consumers, workers, business, and governments of genuine supply chain diversification. This leads to uncertainty within the business community and, frequently, frustration with the inability to distinguish acceptable transnational commerce from activities that policymakers may move to regulate or even prohibit.

To bridge this definitional gap, policymakers in the United States, China, and elsewhere define vulnerabilities from economic interdependence in terms of surveillance and disruption risks. Surveillance risks broadly comprise threats to sensitive data of American citizens, company systems and information, or government activities that may be compromised through interconnected networks that are inherent to transnational business activity. Events like major hacking or cyberthreat incidents push these concerns to the immediate surface, although they are hardly the only threats.

Disruption risks include supply chain disruptions and vulnerabilities as well as concerns that interdependence or economic openness may allow real or potential adversaries to weaponize critical infrastructure or exercise coercive economic leverage over businesses and individuals to a degree that would destabilize the U.S. economy or society. Most companies are familiar with supply chain resilience. The 2021 White House supply chain review report states plainly: “Small failures at even one point in supply chains can impact America’s security, jobs, families, and communities.”⁷⁴ But the connection between what some firms see as everyday global business activity—pushing and pulling software updates through global subsidiaries, connecting and disseminating data through distributed computing systems, transferring production abroad to be closer to markets, and engaging in research and development in locations with high human capital talent pools—can be viewed by governments as engendering serious vulnerabilities and therefore be subject to rapidly changing policies or politicization.

Our research, discussed in the main report in Section II, shows that companies struggle to deal with changing security scopes in the United States and in China. Interviews and survey data, including discussions with government officials in the United States, suggested considerable uptake of third-party verification processes and tools. Table A3.1 categorizes these tools with examples of providers.

Table A3.1: Private and Public Sector Tools for Risk Monitoring and Compliance

Private Sector Third-Party Providers by Function	Public Sector Tools for SCRM
<p>Supply Chain Risk Management (SCRM): Tech-enabled supply chain mapping and company participant due diligence Examples: Exiger, 1nteger (Kharon), Altana</p>	<p>Comply Chain (Department of Labor): Tools and processes to ensure compliance with trade law, focused on forced labor and trafficking</p>
<p>Cyber Supply Chain Risk Management (CSCRM): Software and hardware verification and supply chain identification Examples: ChainSec</p>	<p>Cyber Trust Mark: (Federal Communications Commission) Process to secure voluntary “CyberTrust” label for smart products</p>
<p>Cyber Threat Intelligence (CTI): Custom cyber threat analysis and monitoring Examples: Google (Mandiant), Sekoia, Intel471, Recorded Future</p>	<p>Consolidated Screening List: U.S. International Trade Administration; consolidates screening lists from the Departments of Commerce, State, and Treasury for sanctions or controls</p>
<p>Governance, Risk, and Compliance (GRC): Third party due diligence and screening automation Examples: Navex, Sayari, Wirescreen, Datenna</p>	

⁷⁴ <https://www.bis.doc.gov/index.php/documents/technology-evaluation/2958-100-day-supply-chain-review-report> p. 6.

Annex IV: Research Methodology


The data in the report come from three sources. First, HBS researchers conducted interviews through a convenience sample with personnel from more than 50 firms. Most are headquartered in the United States, but several were subsidiaries of parent companies abroad. The interviews were open ended; we discussed how different firms have experienced risk, what they see as the most significant present and future challenges of business resilience, and how risk management is governed within their organizations. These conversations were not limited to a focus on China; many firms were open about their approaches in other complex geographies, including experiences with Russia pre- and post-2022 sanctions, as well as challenges in new geographies, such as Vietnam and India, in which they seek to diversify their operations. Nonetheless, most firms we spoke with had deep interactions in China, and even highly globalized ones in almost all major international markets seemed themselves primarily focused on China in their political risk thinking.

The group of companies represented in interview data is not representative of the broad population of U.S. firms doing business with or in China or otherwise exposed to China, but the sample includes firms from a variety of sectors and with a variety of levels of exposure in China (see Table A4.1). All interview data are presented anonymously in this report.

Table A4.1: Firms Featured in Qualitative Interviews

Sectors Represented	Modes of Exposure to China
Semiconductors	Joint ventures (JVs)
Financial services	Direct investment in China, including JVs and wholly foreign-owned enterprises (WFOE)
Manufacturing	
Health care (devices)	Portfolio investment in China
Pharmaceuticals	
Consumer package goods	Sell in China
Electrical equipment	Chinese supply chain presence
Telecommunications	Risk from Chinese competitors
Internet services and technologies	Investment from China (direct and portfolio)
Shipping and logistics	Research and development (R&D) in China
Agriculture and commodities	
Oil and gas	Service provision to Chinese companies outside of China
Automotive	
New energy (solar, batteries)	
Consulting and advisory services	
Robotics	
Artificial intelligence	
Mining, critical minerals	

The second and third sources of data comprise two surveys aimed at collecting more systematic data from U.S. companies. One survey was with members of the Chamber of Commerce through Chamber “centers,” divisions within the Chamber to organize companies with common interests. Membership in these centers, like the Chamber generally, is voluntary and initiated by the firms themselves, but these firms tend to be relatively large and globalized. A second source of data comes from a survey of chief legal officers through partnership with the Association of Corporate Counsel (ACC), a nonprofit professional organization of legal officers in enterprises. The ACC has a well-established research function and has generously partnered with HBS and the Chamber Foundation to field the survey with their members who identify as chief legal officers. Respondents from the ACC survey represent a broader array of U.S. firms, including small and medium enterprises as well as the large and global ones that feature more prominently in the Chamber survey.




The survey data collected were anonymous to HBS researchers, although we asked questions about firm demographics, including industry, employee base, and revenues. Substantive responses were common between these two populations, despite their demographic differences. Although response rates were relatively low (n = 40–88 for the Chamber survey and n = 150–189 for the ACC data ranges because not all respondents answered every survey question), we have confidence that the data are not biased by the response rate because we have no reason to believe that response is correlated with any particular viewpoint or experience in geopolitical risk.

Although several convenience surveys of firms on geopolitical risk are in the public domain, most surveys tend to collect data from clients of the advisory groups that publish the data, and therefore oversample resourced firms that are predisposed to be concerned about geopolitical risk. By contrast, the data here, to our knowledge, represent the first effort to collect broad systematic data on how U.S. firms perceive and manage geopolitical risks. In what follows, we display the data from both surveys and discuss deeper knowledge gleaned from interviews. The survey asked a few open-ended questions, and some responses feature in the discussion.

In July–August 2024, the U.S. Chamber of Commerce (USCC) and the ACC each fielded a survey with a sample drawn from their respective lists of contacts at U.S.-based businesses. The goal was to gain insights about geopolitical risk from people who U.S. businesses task with assessing and managing such risk.

The response rate for the USCC survey was 3.5%. The ACC survey response rate was 1.3%. Given these rates and the convenience sampling described here, the survey data are limited in their generalizability. However, the survey respondents constitute an important and difficult-to-reach population—employees working in legal, security, governmental, and international divisions of small and large U.S. companies. This appendix briefly outlines the survey sample and sampling so that the reader can better weigh potential sample biases against the value of reaching an understudied population that works directly on geopolitical risk in U.S. businesses.

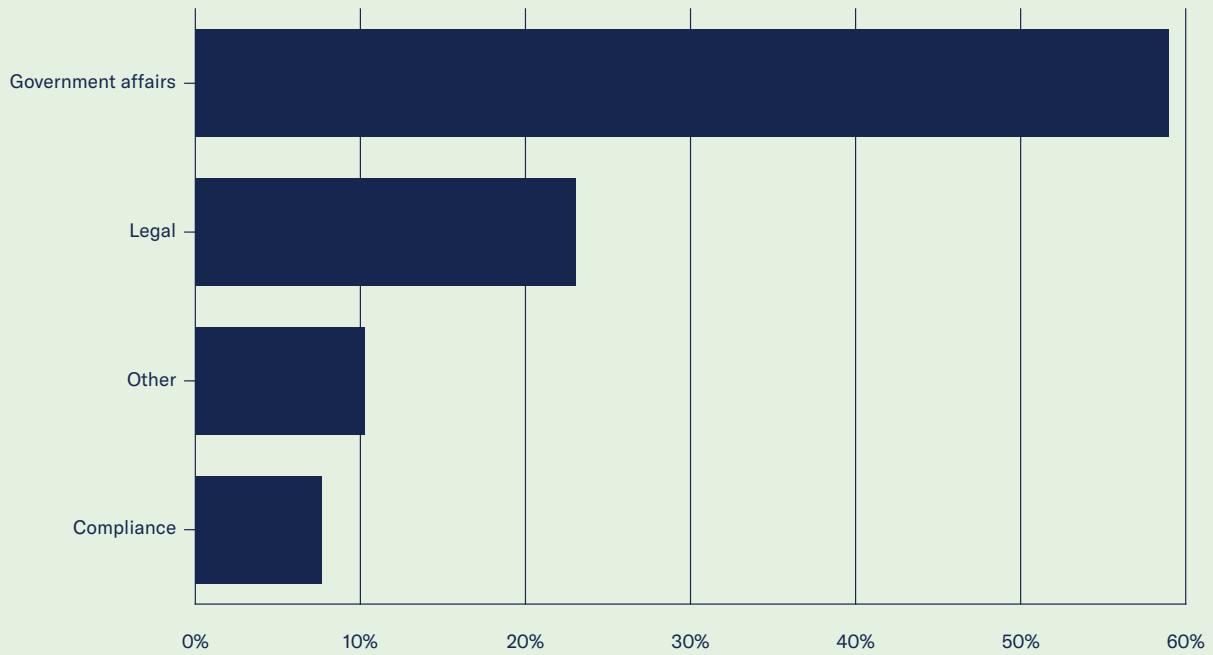


The USCC built its sample frame from topical contact lists that the organization maintains to reach constituents in the American business community. USCC employees used their knowledge of how these lists are created and organized to select lists and contact keywords that would be most likely to yield a sample of employees who work on international business risk. The organization sent survey requests to contacts whose job title included the words “Government,” “Legal,” “General Counsel,” or “Security.” Additionally, contacts from the organization’s international list whose with job titles included “Public Policy,” “Global,” or “International” also received survey requests. Finally, the organization sent survey requests to all contacts from its Cyber Chief Officers list and National Security Task Force lists. Of the 1,701 survey requests that the USCC sent, 88 received responses.

The ACC’s sample frame consisted of current and past members of the ACC who serve as chief legal counsel, general counsel, deputy general counsel, or associate general counsel at U.S. companies. Of the 14,918 survey requests sent by the ACC, 176 received responses. Additionally, the ACC recruited 32 respondents from its online forums, for a total of 208 responses.

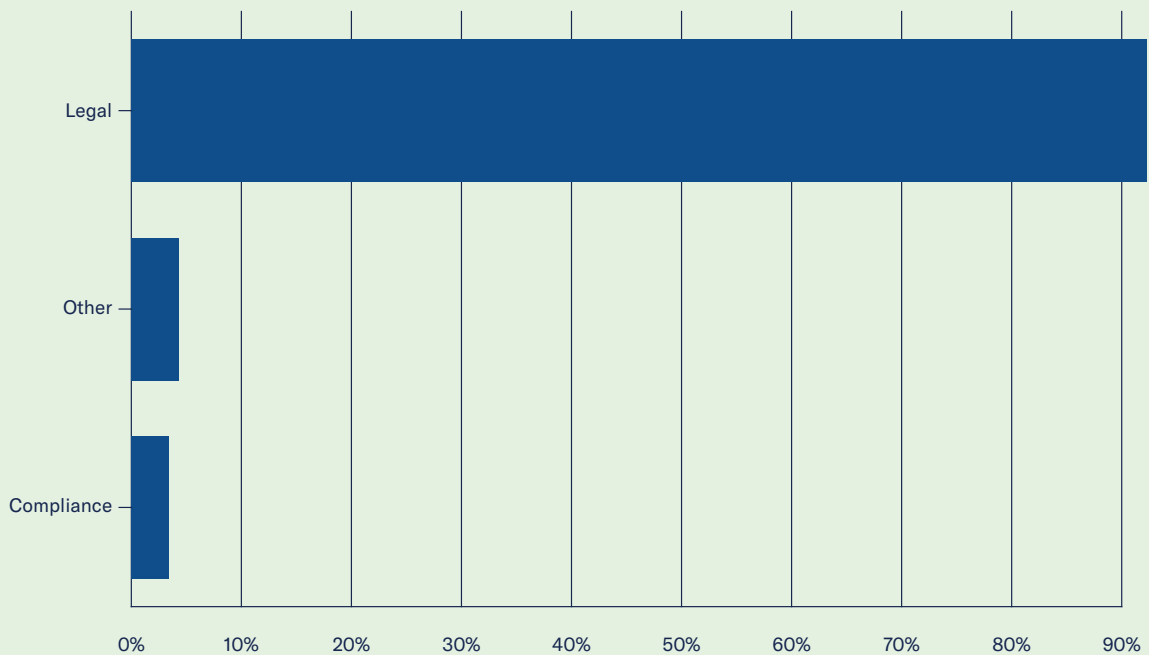
The following figures show the roles of the respondents from each sample, the size of their companies, and the industries of their companies.

Respondent's Role in Company, USCC



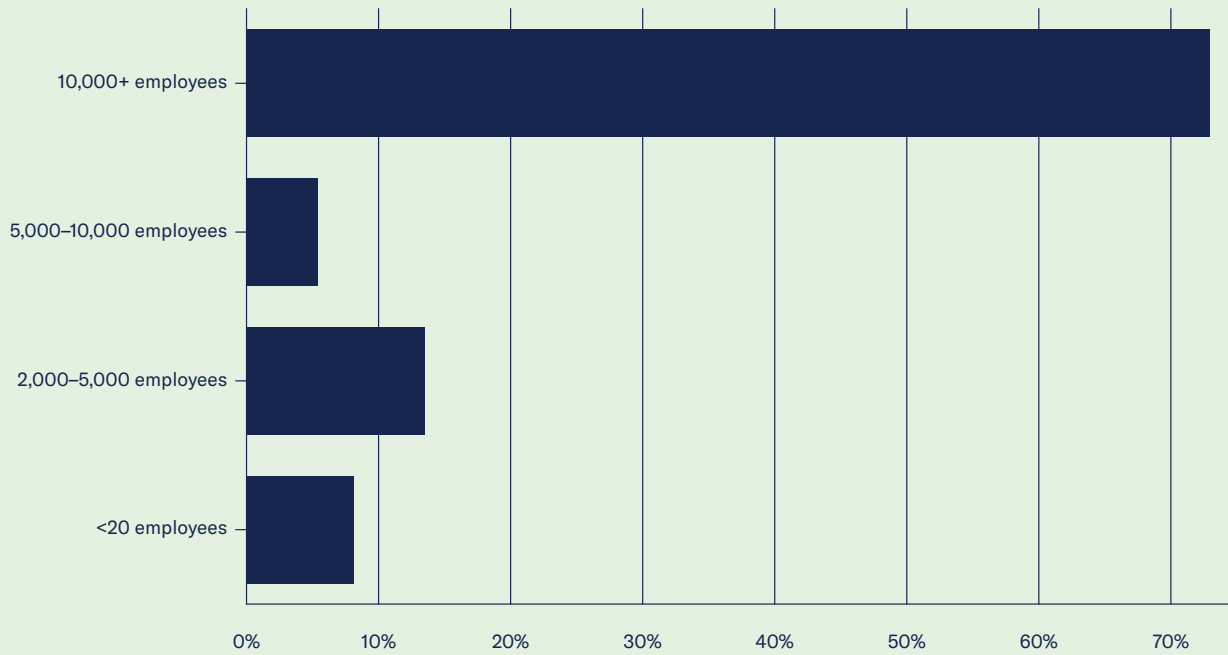
Data are from survey conducted August 2024. Data include 39 responses.

Respondent's Role in Company, ACC



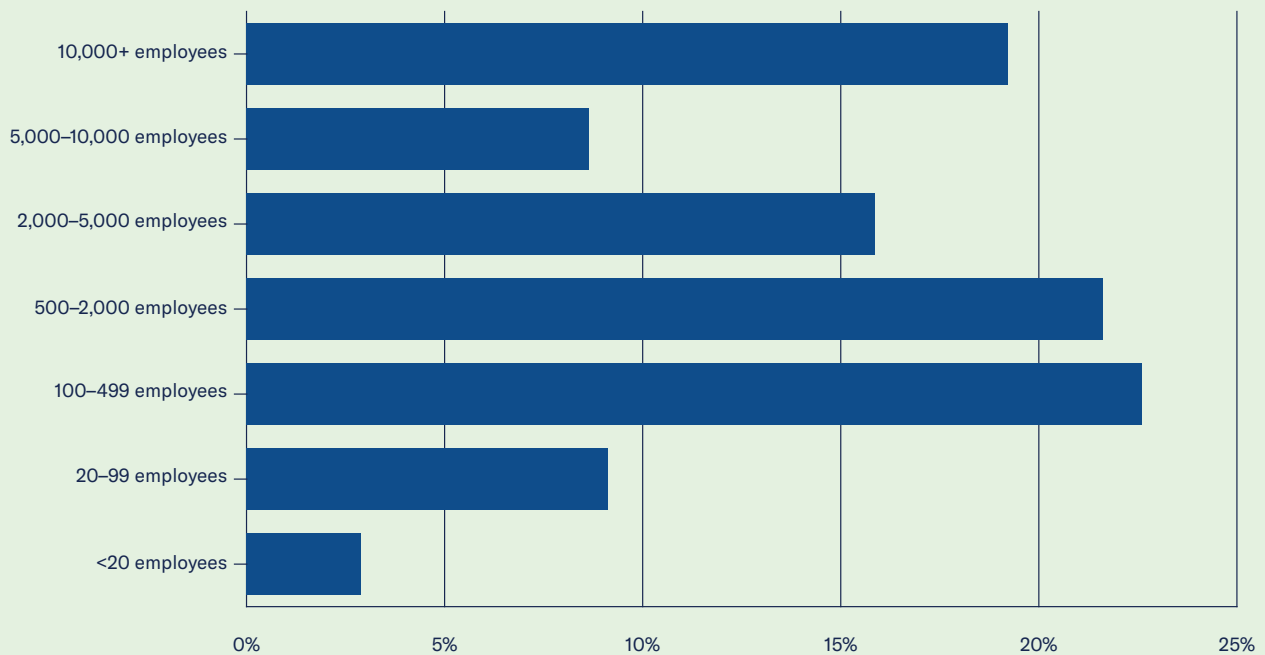
Data are from survey conducted August 2024. Data include 208 responses.

Number of Employees at Respondent's Company, USCC



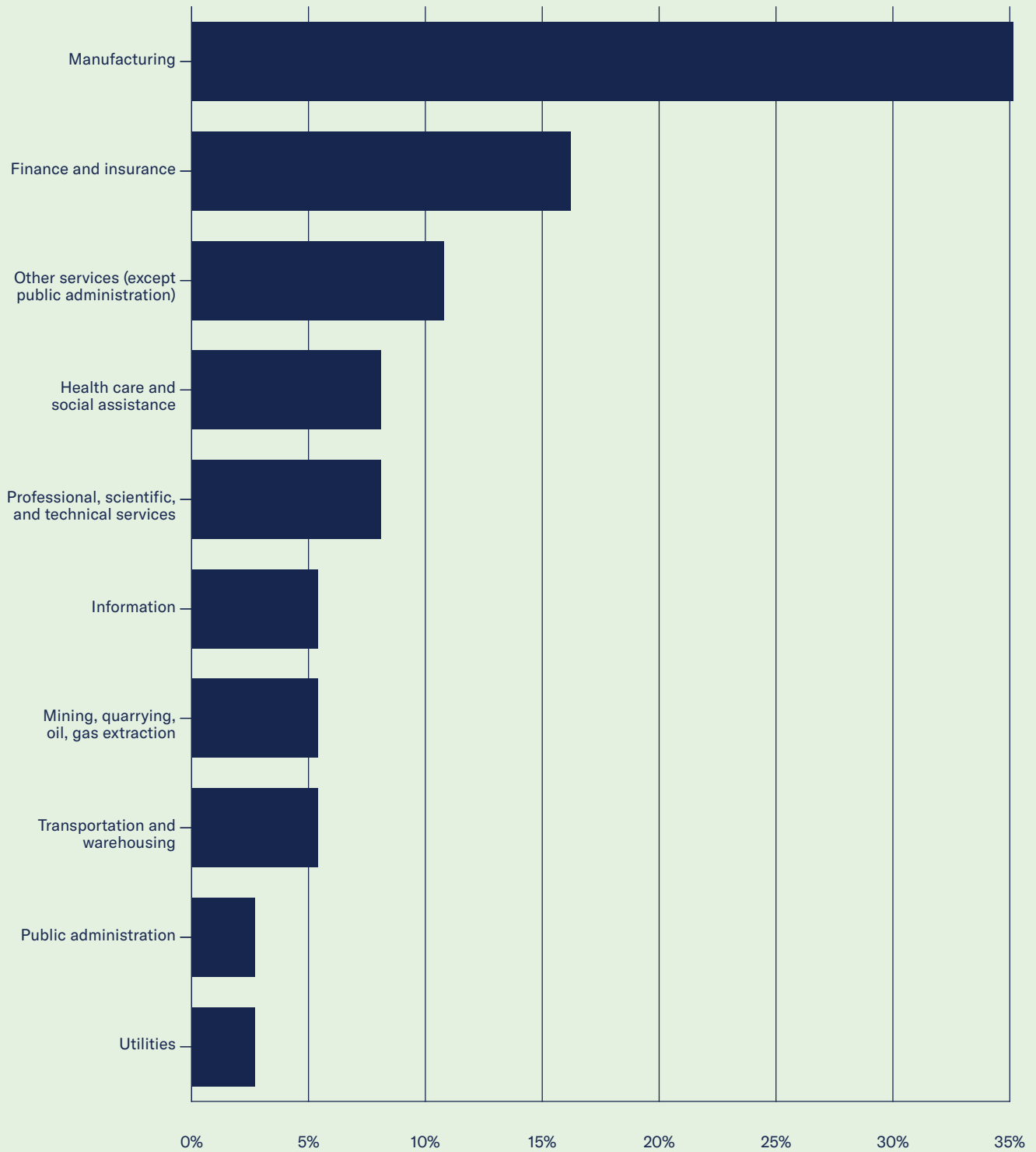
Data are from survey conducted in August 2024. Data include 37 responses.

Number of Employees at Respondent's Company, ACC



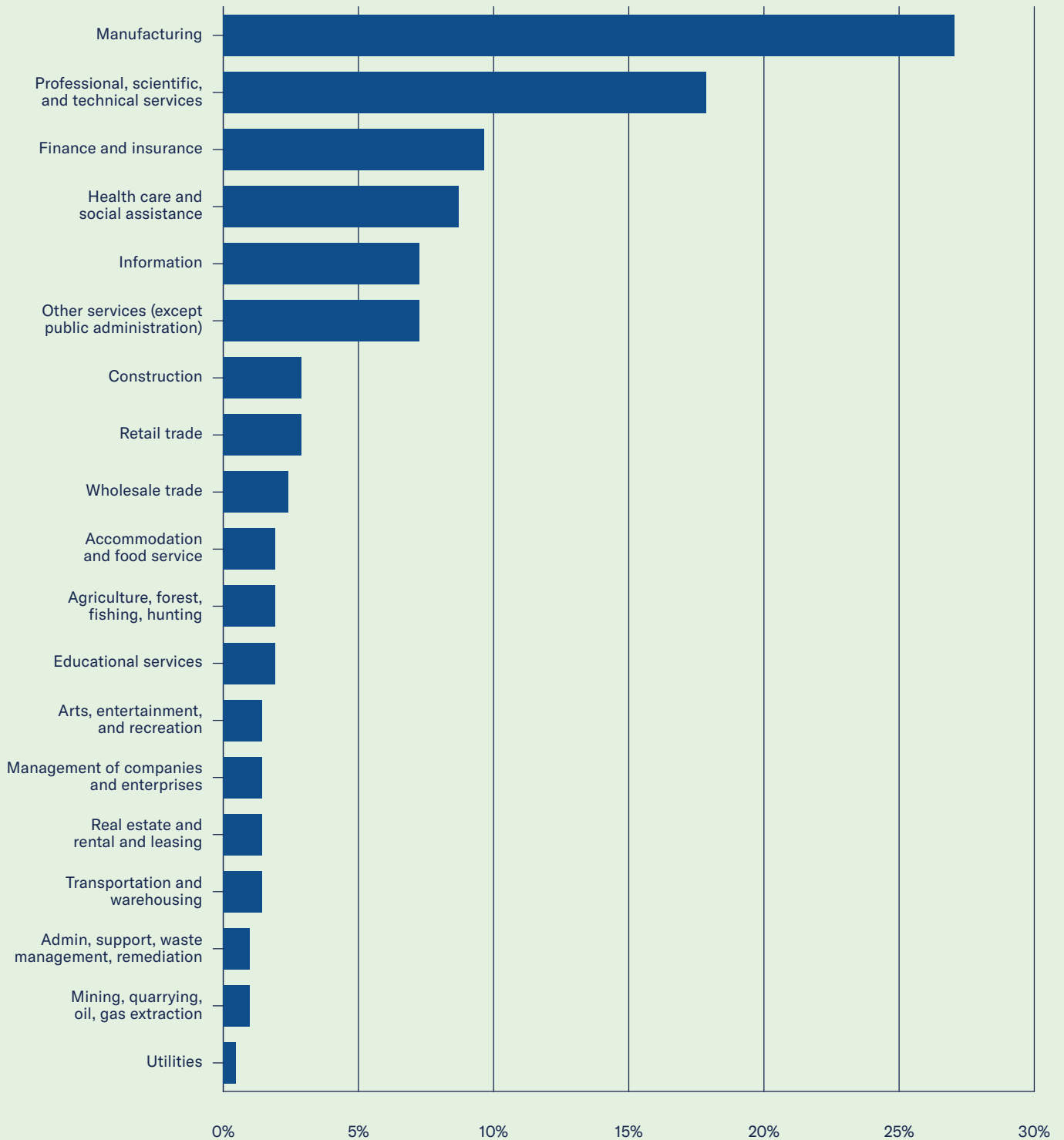
Data are from survey conducted in August 2024. Data include 208 responses.

Respondent's Role in Company, USCC



Data are from survey conducted in August 2024. Data include 37 responses.

Industry of Respondent's Company, ACC



Data are from survey conducted in August 2024. Data include 207 responses.



U.S. Chamber of Commerce
Foundation