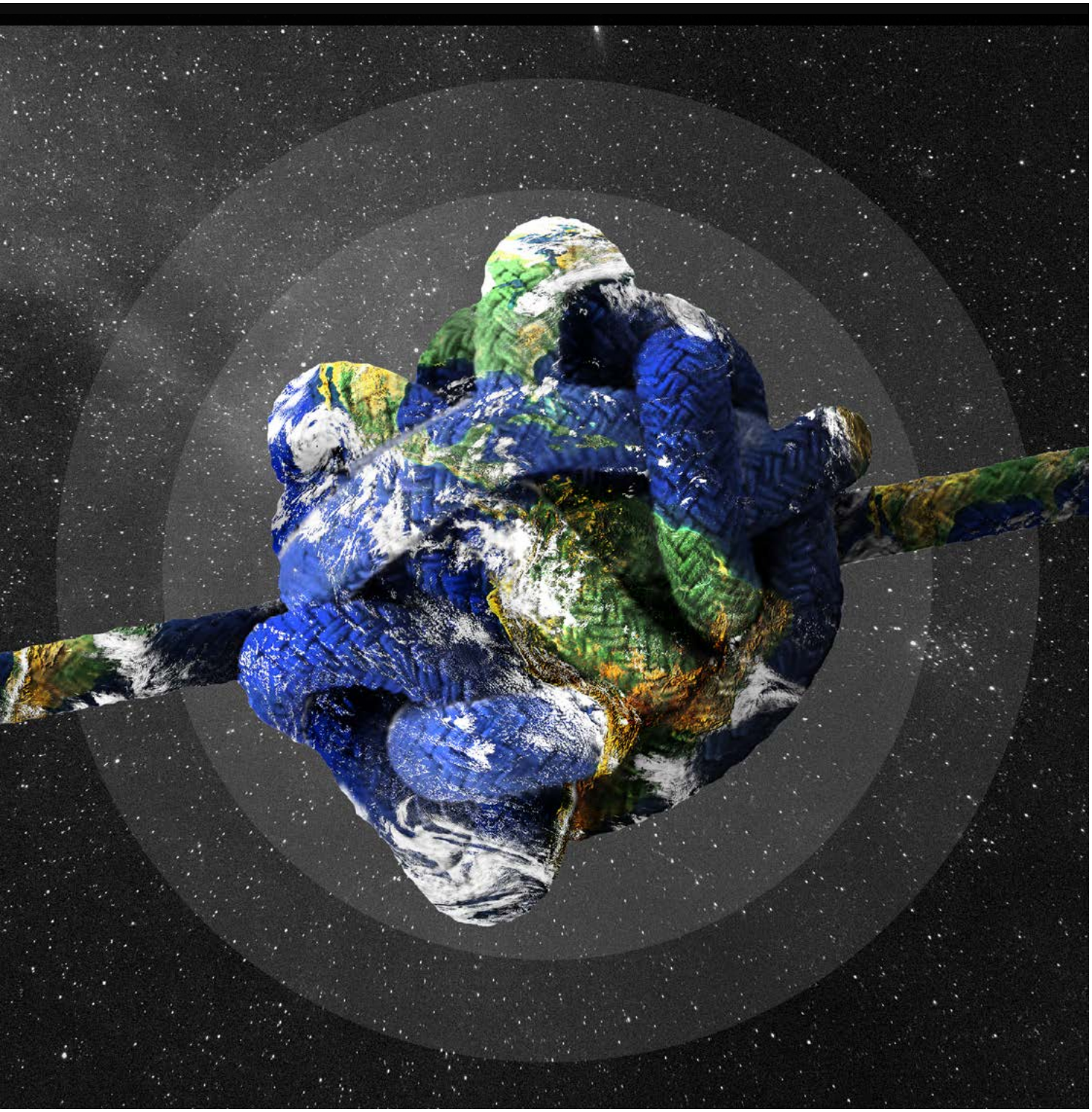
MARCH 2022

The Tangled Web We Wove

Rebalancing America's Supply Chains

Megan Lamberth, Martijn Rasser, Ryan Johnson, and Henry Wu



CNAS

About the Authors

Megan Lamberth is an Associate Fellow for the Technology and National Security Program at the Center for a New American Security (CNAS). Prior to joining CNAS, she was a Brent Scowcroft fellow with the Aspen Strategy Group, where she helped spearhead the planning and execution of the Aspen Strategy Group's Summer Workshop and two sessions of the Aspen Ministers Forum. She received her MA in international affairs from the Bush School of Government & Public Service at Texas A&M University. She graduated from Sam Houston State University with a BA in criminal justice.

Martijn Rasser is Senior Fellow and Director of the Technology and National Security Program at CNAS. Previously he served as a senior intelligence officer and analyst at the Central Intelligence Agency. Upon leaving government service, Rasser was chief of staff at Muddy Waters Capital, an investment research firm. More recently he served as director of analysis at Kyndi, a venture-backed artificial intelligence (AI) start-up. Rasser holds a BA in anthropology from Bates College and an MA in security studies from Georgetown University.

Ryan Johnson is the Joseph S. Nye Jr. Intern for the Technology and National Security Program at CNAS. He recently graduated summa cum laude from the U.S. Military Academy at West Point, majoring in American politics. During his senior year at West Point, Johnson served as the honor executive officer, overseeing the day-to-day operations of the Cadet Honor Committee and assessing the effectiveness of the cadet leader development model. Johnson also was a Presidential Fellow through the Center for the Study of the Presidency and Congress and published his original research in its annual journal.

Henry Wu is a former Joseph S. Nye Jr. Intern for the Technology and National Security Program at CNAS. He previously interned at the Center for Strategic and International Studies, focusing on global supply chains, international trade, and the implications of emerging technologies for human rights and sustainability. Wu is currently working on an MPhil in politics at the University of Oxford, where he studies as a Rhodes Scholar. He holds a BA in philosophy and political science from the Ohio State University.

About the Technology and National Security Program

Technology is changing our lives. Rapid developments in AI, autonomy and unmanned systems, digital infrastructure, networking and social media, and disinformation are profoundly altering the national security landscape. Nation-states have new tools at their disposal for political influence as well as new vulnerabilities to attacks. Authoritarian governments are empowered by high-tech tools of oppression and exploit radical transparency. AI and automation raise profound questions about the role of humans in conflict and war. CNAS' Technology and National Security Program explores the policy challenges associated with these and other emerging technologies. A key focus of the program is bringing together the technology and policy communities to better understand these challenges and together develop solutions.

Acknowledgments

The authors are grateful to Brandon Daniels, Andrea Little Limbago, and James Mulvenon for their valuable feedback and suggestions on the report draft. A special thanks to all those who participated in our Securing America's Critical Supply Chains roundtables. Your insights helped shape the ideas and analysis in this report. The views expressed in this report are those of the authors alone and do not represent those of the roundtable participants.

We also would like to thank Govini and Interos for allowing us to use their data and graphics. Thank you to CNAS colleagues Maura McCarthy, Melody Cook, Rin Rothback, Emma Swislow, and Anna Pederson for their role in the review, production, and design of this report. Any errors that remain are the responsibility of the authors alone. This report was made possible with general support to the Technology and National Security Program.

TABLE OF CONTENTS

Executive Summary

The pendulum of globalization has swung too far. What the fallout of the ongoing pandemic makes clear is that decades of offshoring and cost-cutting in the pursuit of efficiency and a better bottom line have left the supply chains of the United States and its allies and partners unacceptably brittle. Restoring balance to the system—with greater resilience through reducing dependence on potential adversaries, greater geographic diversity, and a pragmatic approach to building a mix of domestic capabilities and sourcing from reliable partners—will be a complex, expensive, and far-reaching undertaking. It could well reshape the global economy and strengthen ties between the world's democracies, and is likely to be a key factor in determining the course of the global strategic competition.

Tackling America's supply chain problems will require a new conceptual framework that is fit for the current geopolitical context. The United States and China are engaged in a complex economic, political, and military competition marked by sharp ideological and normative differences and economic dependencies. Global trade and supply chain dynamics reflect much of the spectrum of this competition, the overreliance on China for key inputs and manufacturing capacity most prominently. Correcting this imbalance and assuring the resilience and security required is needed to ensure long-term American competitiveness.

The framework with which to address that imbalance has three core elements: adjusting the role of government, checking the key assumptions that shaped current global supply chains, and balancing the tension between self-reliance and interdependencies. Policymakers and business leaders alike must rethink how government and industry engage each other on supply chain matters as part of a new form of industrial policy. For example, government officials need to better understand global supply chains to identify vulnerabilities and pursue opportunities. At the same time, company officers must strive for greater transparency and continuous supply chain assessments.

Restoring balance will require a new approach to thinking about the trade-offs between efficiency, reliability, availability, and security. No longer will the least expensive supply chain option necessarily be the most effective, nor will the highly optimized one always be the most desirable. Supply chain resilience often will require geographic diversity and surge capacity, principles that may clash with a company's near-term bottom line.

Finally, a balance must be struck between the understandable desire to be self-sufficient and the realities of cost and feasibility. In most cases, autarky would be prohibitively expensive and not achievable because of the global diffusion of raw materials, technologies, know-how, and manufacturing capacity. Instead, policymakers should consider how to leverage allies and partners to establish more robust and secure supply chains.

This report offers a schema to help U.S. decision makers navigate those trade-offs by categorizing factors of necessity and geography. Using this schema as a baseline, government and industry leaders can shape a blueprint for remapping supply chains. The report then builds on that basic framework by offering specific actionable policy recommendations to ensure that the resulting U.S. supply chain strategy is comprehensive, proactive, and achievable.

Tackling America's supply chain problems will require a new conceptual framework that is fit for the geopolitical context.

To promote more resilient and secure supply chains, the U.S. government must enact a range of policy actions. Cooperation with industry and allied and partner countries should be an essential feature of this strategy. The following recommendations comprise specific actions focused on bolstering the government's ability to manage supply chains through greater organizational capacity and authorities. Also proposed are investments and initiatives that are likely to transform supply chains to the long-term benefit of U.S. national and economic security.

Manage Supply Chains

The White House, with the support of Congress, should:

- *Craft a supply chain strategy.* The United States needs a blueprint for how to think about, and prioritize, the security and resilience of its critical supply chains.
- *Remap critical supply chains.* Many supply chains important to U.S. economic security and national defense are dangerously brittle. Addressing these vulnerabilities will be expensive, complex, and time consuming. The risks of not restructuring these supply chains, however, are even greater.
- *Institutionalize supply chain reviews.* The U.S. government should institutionalize the use and frequency of supply chain reviews for critical sectors as part of a comprehensive framework to monitor and continuously improve supply chain resilience efforts.

- *Engage with industry leaders and private sector partners on the development and implementation of supply chain restructuring.* Policymakers and government officials must continue to engage private sector partners and leverage existing models of public-private partnerships when considering the restructuring or remapping of critical supply chains.
- Leverage existing federal legislation and regulations to incentivize and drive transformation beneficial to the U.S. economy and defense. U.S. executive agencies have the authority to enforce, as well as regulate through supervision authorities in critical infrastructure, critical sectors related to U.S. defense or economic security.

Congress, in consultation with relevant government agencies, should:

- *Expand the use of existing industrial survey authorities.* The Department of Commerce's Bureau of Industry and Security (BIS) has the authority under section 705 of the Defense Production Act to conduct "industry studies assessing the U.S. industrial base to support the national defense."[1]
- *Promote efforts to improve software supply chain security.* Existing governmental efforts to strengthen the resilience of supply chains should acknowledge and address software supply chain security.
- *Evaluate vulnerabilities in U.S. stockpiles of critical materials and supplies for national defense.* The U.S. government must prepare its strategic stockpiles for widespread disruption to global supply chains by increasing funding and resources for emergency preparedness and response.
- *Encourage relevant government agencies to adopt emerging technologies, such as blockchain, to build transparency and accountability*. Distributed ledger systems ensure transparency for all parties along a given supply chain by providing verifiable and certified information at every level of production.
- *Identify, develop, and apply security principles for technologies in supply chains*. As private industry continues to adopt emerging technologies such as 5G and Internet of Things infrastructure, cybersecurity concerns remain a persistent threat.[2] Congress in consultation with the Federal Communications Commission should review relevant principles for ensuring safe and secure usage of these technologies throughout critical supply chains.
- *Review and amend outdated provisions in the Uniform Commercial Code and others to optimize supply chain coordination*. The governing legal standards for supply chains in the United States are based on the privity of contract doctrine, which prevents external parties and individuals from enforcing the obligations of a contract they are not a part of.

Transform Supply Chains

Congress should:

- *Expand the mission of the Bureau of Industry and Security.* BIS should assume authority to regulate and protect U.S. technology supply chains. It should be reorganized to model the Department of the Treasury's Office of Terrorism and Financial Intelligence.[3]
- *Create an assistant secretary of commerce for supply chain and technology security.* This position would centralize the department's policy and regulatory programs involving supply chain integrity, availability, and resilience, such as Defense Production Act programs, and planning and administration of BIS industry surveys.

Congress, in conjunction with the State Department and the White House, should:

- *Establish a network of like-minded countries to collaborate on technology policy.*[4] Technology policy coordination among like-minded countries is often sporadic and disjointed. The United States should create a multilateral technology alliance with a core group of like-minded countries to collaborate on supply chain diversification.[5]
- *Bolster U.S. capacity to conduct tech diplomacy.* The United States needs a robust tech diplomacy capability to address the international dimensions of supply chains and technology competition more broadly.

The Department of Commerce should:

- Establish an information fusion center, headquartered in the International Trade Administration's Office of Industry and Analysis. Anticipating and mitigating supply chain risk will require a permanent and dedicated effort to monitor and analyze developments in industry and actions by foreign governments that impact supply chain dynamics.

The National Science Foundation, in collaboration with relevant agencies, should:

- *Invest in next-generation tools, platforms, and technologies for supply chain security.* For example, AI tools hold great promise to improve supply chain management such as by analyzing vast data sets, enhancing understanding of relationships, and supporting decision-making.

Introduction

Supply chains are a pillar of American economic advantage, national security, and long-term technological leadership. Secure, dependable, and resilient supply chains are essential for U.S. competitiveness and the day-to-day functioning of society, particularly in high-tech areas such as advanced semiconductors, and critical sectors including pharmaceuticals and medical equipment.

Ensuring secure supply chains, however, is no easy task. The United States must thread the needle on free market principles and government intervention in the economy, while striking a balance between self-reliance and international partnership, and calibrating between investments in proven capabilities and possible game-changing innovations.[6]

Modern supply chains are vast, complex, and global. While they always have been afflicted with certain vulnerabilities, the fragility of supply chains has been on full display in recent years. Supply chains have been stretched thin by a number of factors, some more long-standing than others. As the scale and complexity of the supply chain issue is vast, it helps to diagnose the problem through the lens of three C's that make supply chain resilience the challenge it is today: coronavirus, China, and climate.

The COVID-19 pandemic exposed the widespread brittleness of global supply chains and the risks of achieving economies of scale by concentrating production in small geographic areas. By placing pressure on the U.S. healthcare and pharmaceutical sector, the pandemic exposed vulnerabilities in critical sectors, and raised questions about America's ability to effectively function during a prolonged crisis.

Some of these vulnerabilities were pandemic induced—countries around the world were suddenly confronted with shortages of essential medical gear and medicines. Other vulnerabilities are long standing. China's stranglehold over the rare earths sector, for example, presents serious vulnerabilities for innovations essential to military preparedness and the competitiveness of America's domestic industry. America's adversaries are poised to take advantage of supply chain dependencies to potentially threaten U.S. national security and economic competitiveness.

China looms large. Where the pandemic exposed numerous near-term constraints—many rooted in the country's centrality in global supply chains—over the long haul the U.S. government must deal with China in the context of a long-term geopolitical competition. Here the chief concern is how to disentangle critical supply chains where the United States is vulnerable to disruptions because of a high reliance on China, such as for critical minerals, and how to shift certain production lines out of China without causing major disruptions to private industry in the United States and allied countries.

Climate change is a third vexing challenge. There will be events that will be difficult to anticipate and unfolding trends whose effects researchers are only beginning to think through. The long-term implications of climate change are not yet fully known or understood but already are being felt around the world. A drought in Taiwan and an enormous winter storm in Texas impacted semiconductor fabrication; extreme weather events, expected to become more common as the climate changes, are likely to affect food security. At the same time, a warming Arctic is opening up new shipping lanes and making Greenland a more attractive place for rare earths mining—presenting opportunities and likely new geopolitical flashpoints. Climate and geography must be part of the supply chain resilience and security equation.

The U.S. government is taking steps to improve the resilience of America's supply chains. Recent reports, from the bipartisan House Armed Services Committee Defense Critical Supply Chain Task Force and the White House (pursuant to Executive Order 14017) have underscored the importance of supply chain security.[7] But more work is needed.

Improving the resilience of America's supply chains will be an iterative process. As emerging technologies—such as AI, biotechnology, and additive manufacturing—redefine the landscape of innovation and geostrategic competition, new approaches to ensuring secure and resilient future supply chains are needed.

This report explores the vulnerabilities impacting America's supply chains and offers a framework for how to address those vulnerabilities, as well as ones that may manifest in the future. The report also examines case studies of two critical but differing sectors—the semiconductor supply chain and the software supply chain—which provides context for determining effective actions for improving resiliency. Finally, the report offers a series of policy recommendations meant to help guide and strengthen the U.S. government's response to supply chain security.

The breadth and complexity of modern supply chains can make the challenge of securing and strengthening them seem elusive and unreachable. While a universal solution to addressing supply chain vulnerabilities may not exist, there are concrete steps the United States can take to make its supply chains less brittle, particularly those most critical to its economic security and defense. More needs to be done—and urgently so—to ensure that U.S. supply chains are fortified against whatever upheaval they might face in the future.

SUPPLY CHAIN CONCEPTS

Risk Management
Supply chain risk management is the continuous process of monitoring and analyzing supply chain risks—such as the integrity and availability of a raw material, component, or software—and implementing management, operational, and technical controls to address those risks.[8]

Resilience
Supply chain resilience refers to the capability to mitigate and recover from a disruption. These disruptions can be natural, such as an earthquake, tsunami, or pandemic; or deliberate, such as a country intentionally withholding a key input.

Concentration Risk
Supply chain concentration risk can take numerous forms (lack of vendor diversity, geographic, financial) but all share the basic quality of excessive reliance that could lead to a single point of failure.

Sourcing
Supply chain sourcing "is the process of vetting, selecting, and managing suppliers who can provide the inputs an organization needs for day-to-day running. Sourcing is tasked with carrying out research, creating and executing strategy, defining quality and quantity metrics, and choosing suppliers that meet these criteria."[9]

Auditing
Supply chain auditing is the process of examining supply chains for risks, inefficiencies, reliability, and compliance among other motivations. From a national and economic security standpoint, auditing is generally referred to in the context of identifying risks such as those from geopolitical and geotechnical tensions, lack of vendor diversity, lack of transparency, and single points of failure.

Compliance
Supply chain compliance refers generally to organizational adherence to laws, regulatory or contractual requirements, and guidelines.

Tier 1 and Tier N Suppliers[10]
Suppliers that make up a particular supply chain can be broken down into different tiers. Tier 1 suppliers conduct business directly with the original equipment manufacturer. Tier N suppliers serve as the primary sources of materials and component parts for preceding tiers. As a result of hyperspecialization, many supply chains contain a multitude of tiers.

"Just In Time" Model[11]
A supply chain management framework that seeks to reduce production time and costs by minimizing inventories across the entire supply chain. This model increases the return on investment by improving product quality and lowering costs by reducing overhead. It can be crippled, however, by sudden changes in supply or demand.

Key Supply Chain Vulnerabilities

The COVID-19 pandemic has caused world-wide disruptions in supply chains, revealing widespread and interrelated vulnerabilities. Some of these vulnerabilities are long-standing challenges, while others manifested more recently as supply chains were thrown in disarray from country lockdowns, factory shutdowns, and long-term travel restrictions.

This section covers the five most pressing vulnerabilities impacting U.S. supply chains. The first vulnerability is America's reliance on peer competitors, particularly China, which opens the door to unfavorable control and influence. U.S. dependence on China for critical inputs, such as rare earths, puts the country's national security and economic security at risk. The second is the brittleness of global supply chains. Popular manufacturing models, especially the "Just in Time" model, prioritize speed and cost-effectiveness over security and resilience, which can result in disruption at all levels of the supply chain.

> **Each of these vulnerabilities has a unique impact on global supply chains, but they also are interconnected in many ways.**

The third vulnerability impacting supply chains is geography. Manufacturers must prepare for the unexpected, including natural disasters, extreme weather events, and geopolitical tension which create potentially outsized effects. Fourth is a lack of vendor diversity. Products that require materials from a certain region or a single source are more at risk for disruption. The fifth vulnerability is limited transparency, which poses a risk to today's complex and interconnected supply chains.

Each of these vulnerabilities has a unique impact on global supply chains, but they also are interconnected in many ways. While the COVID-19 pandemic did not generate these vulnerabilities, it certainly exacerbated them, leading to reduced manufacturing, worker shortages, bottlenecks, and wide-ranging shortages. As the United States and the rest of the world recover from the damaging economic impact of the pandemic, a concerted and strategic effort must be made to resolve these issues and build a better, more resilient system of supply chains.

Reliance on Adversarial Competitors

U.S. supply chains are vulnerable from overreliance on adversarial competitors, namely China. This overreliance creates opportunities for undue influence on American and allied manufacturing capabilities by controlling and weaponizing supply chain choke points. This vulnerability developed as a result of the three decades–long trend toward globalization and open markets. Although the structural weaknesses of globalized supply chains were recognized even during its adoption throughout the late 20th century, the strategic implications were felt most immediately during the COVID-19 pandemic and crystallized as policymakers grasped the scope and scale of the challenge of a rising China.[12] Because these risks and realities are inherent to the current supply chain structure, mitigating and controlling this vulnerability must be a critical national security focus area.

The evolution of the modern supply chain was motivated by the optimistic belief in liberal economic interdependence theory and globalization. According to this camp, a globalized and dispersed world economy paired with outsourcing of domestic production and services would facilitate increased trust among would-be competitors and incentivize cooperation.[13] Trade expectations in turn would foster further international stability and improve the global quality of life. Throughout the 1990s, domestic manufacturers outsourced their labor and production supply chains abroad, resulting in lower costs for consumers and increasing economies of scale for industry.[14] Proponents of this theory also believed economic interdependence would bring peace between countries and incentivize authoritarian states to prefer free markets as opposed to state intervention.

This globalized interdependence theory undergirded many economic decisions for the next three decades. Most noticeably was China joining the World Trade Organization (WTO) in 2001. As President Bill Clinton argued at the time, "By joining the WTO, China is not simply agreeing to import more of our products, it is agreeing to import one of democracy's most cherished values: economic freedom."[15] But as recent events stemming from, and exacerbated by, the COVID-19 pandemic show, there are significant and widespread vulnerabilities underlying this excessive dependence. Adversarial competitors recognize and are leveraging these structural weaknesses to accomplish their own national security aims at the expense of the United States. As of early 2022, America is just beginning to formulate how to mitigate these risks.

Relying on an adversarial competitor, especially a rising power such as China, carries significant undesirable risks that far outweigh the benefits. Overreliance creates an opening for adversarial nations to use this dependency as a tool for coercion. For example, during the initial wave of COVID-19 infections in early 2020, stockpiles of critical personal protective equipment and medical technologies like ventilators rapidly disappeared and became impossible to procure due to global shutdowns and bottlenecks. Coinciding with this rapidly increasing demand, factories went cold due to lockdowns, which halted the production of new materials and supplies. Additionally, critical transportation nodes rapidly became congested, stopping finished products from reaching their destinations.

Throughout the COVID-19 pandemic, ventilators were a critical tool to help patients fight off infection and work toward recovery. During the initial waves of hospitalizations, U.S. hospitals lacked access to these vital technologies, enabling adversarial nations, such as China, to leverage their domestic stockpiles. (Getty Images)

This increased demand, paired with production shortages, enabled states with sufficient supply to exercise influence over those who lacked the ability to produce their own medical equipment. Specific components manufactured in China that were used in ventilators and other essential medical equipment were withheld from the United States and other nations to ensure China maintained its own domestic supply and to exercise leverage

on near-peer competitors.[16] Now, two years after the initial waves of the pandemic, China still exerts this control over other nations and is able to use its supply of medical equipment as a valuable bargaining chip.

At the height of the pandemic, Chinese state-run news agencies noted the regime's ability to cut off pharmaceutical exports in an effort to exert control over foreign competitors.[17] Early last year the Chinese Ministry of Industry and Information Technology proposed export controls on rare earth minerals used in advanced military technology wielded by the United States.[18] While Beijing ultimately did not use these tactics, the risk of future escalation resulting in retaliatory supply chain disruptions is an advantage China can leverage over the United States when it sees fit.

Brittleness

The brittleness of modern supply chains makes them particularly vulnerable to disturbances. This fragility stems in part from opacity, single points of failure, and the growing complexity and interconnectedness of today's supply chains.

This brittleness is further exacerbated by the dominance of manufacturing models that prioritize cost-saving measures over security and resilience.[19] These policies—often referred to as a "Just in Time" model of manufacturing—operate on the idea that materials or parts should be delivered only once they are required, reducing the need for stockpiling.[20] Conceptualized by Japanese auto manufacturer Toyota in the early 1970s, "Just in Time" became a dominant model of manufacturing in the decades that followed for an array of industries, such as automotive, healthcare, clothing and textiles, and electronics sectors. Researchers studying American manufacturing companies found that from 1981 to 2000, inventories were reduced by an average of 2 percent per year.[21] This lean style of manufacturing led to obvious benefits—reduced costs, the ability to more rapidly shift to market demands, and fewer obsolete products.[22] While the advantages are apparent, the model suffers from fragility and inflexibility when disruptions inevitably occur.

Upheavals associated with the pandemic since early 2020 have revealed weaknesses in the "Just in Time" model that have proven lasting and difficult to address. The impact of the COVID-19 pandemic sent shock waves through global supply chains. Medical supplies like masks and ventilators were in short supply, and a shortage of semiconductors impacted countless products from automobiles to game consoles to smartphones.[23] A July 2020 survey from McKinsey found that 73 percent of supply chain executives surveyed had encountered problems with their supplier base, and 75 percent had experienced problems with production and distribution.[24]

A shortage of semiconductors hit the auto industry particularly hard. Early in the pandemic, automakers anticipated limited demand from consumers and canceled their orders of semiconductors. Semiconductor foundries replaced those orders with demand from other industries, leading to a shortage of available chips.[25]

The chip shortage is exacerbated by an overall fragmentation of the supply chain, which makes it difficult for automakers to determine the source of bottlenecks.[26] As White House economic advisors Susan Helper and Evan Soltas explain, "a semiconductor may be designed by one firm, manufactured by a second firm, embedded into a component (such as an air bag) by a third supplier, and only then delivered to an automaker's assembly plant."[27]

The financial impact of these shortages is profound for the auto industry. AlixPartners, an industry consulting firm, estimated the chip shortage would cost automakers upwards of $210 billion in lost revenues for 2021.[28] In July 2021, Ford Motor Company announced its profit for the three preceding months had dropped by 50 percent.[29] Toyota—the company given credit for initiating the "Just in Time" method of manufacturing—announced in August 2021 that it would cut production worldwide by 40 percent for the month of September, citing "Covid-19 and unexpected events with our supply chain."[30] Recently, automakers supply chain woes were further exacerbated by protests in Canada that disrupted some of the U.S. and Canada's busiest trade routes.[31]

Some industries that rely on the "Just in Time" model are learning from this period of upheaval by shifting to a "Just in Case" model. As Brooke Masters and Andrew Edgecliffe-Johnson explain in the *Financial Times*,

> Some businesses are increasing the inventory they keep on hand and entering into longer term contracts with key suppliers. Others are diversifying their manufacturing to create regional hubs with local suppliers and investing in technology to give them greater advance warning of potential bottlenecks. Some companies are also investigating ways of working with their rivals to share information to develop emergency back up facilities without falling foul of competition regulators.[32]

While companies likely will continue to function with a manufacturing model that is lean and prioritizes efficiency, many are finding better ways to prepare their services and products for inevitable, and potentially lasting, supply chain disruptions in the future.

Geography

Industries must account for a variety of potential supply chain disruptions emanating from forces outside of their control, such as natural disasters, extreme weather events, or geopolitical conflict. This risk of geographic concentration affects certain industries and products more than others. The semiconductor supply chain, for instance, is particularly vulnerable because of the concentration of certain materials (e.g., silicon wafers, specialty chemicals, manufacturing equipment) in specific regions around the world, particularly China and East Asia.[33] A report from the Semiconductor Industry Association (SIA) found that "there are more than 50 points across the [semiconductor] value chain where one region holds more than 65 percent of the global market share."[34] This concentration makes the semiconductor supply chain especially vulnerable to geopolitical tension or natural disasters.[35]

Supply chains are not only vulnerable to geographic concentrations but are also susceptible to disruption from natural disasters. While industries always have had to prepare for extreme weather events, this kind of disruption only will increase as the effects of climate change result in more disasters, such as hurricanes, wildfires, floods, and droughts. Global supply chains have been rocked by natural disasters in the past. For instance, the massive earthquake and tsunami that struck Japan in 2011 upended the Japanese auto industry—forcing automakers to shut down assembly plants for weeks and causing ripple effects across the global supply chain.[36] Hurricane Ida, which devastated the Gulf Coast of the United States in 2021, weakened an already brittle global supply chain by exacerbating shortages and shipping delays.[37] Wildfires in Canada and the West Coast of the United States in 2021 caused major challenges for the lumber industry.[38] A massive drought in Brazil—the worst in over a century—caused the price of coffee futures to nearly double what they were a year prior.[39] A massive and unprecedented freeze in Texas in February 2021 led to global shortages in the raw materials used to make a variety of plastic products.[40] The rising frequency of these events will pose greater challenges to supply chain management, particularly to supply chains located in parts of the globe more vulnerable to shocks.

Industries also may face disrupted supply chains as a result of accidents. For instance, in March 2021 the Suez Canal was blocked for almost a week by a giant container ship, which obstructed the primary trade route linking Asia and Europe, resulting in supply chain disruptions around the globe and tens of millions in lost revenue. As much as $10 billion of cargo a day was stalled, including oil, electronics, home goods, and automobiles.[41] The Suez Canal crisis put further strain on a global supply chain already reeling from the pandemic and subsequent shortages. The blockage was a reminder that geography is still a factor in the security and resiliency of supply chains.[42]

Lack of Vendor Diversity

The COVID-19 pandemic revealed the brittleness of certain industries' supply chains. Part of that brittleness stems from manufacturers that depend on a single supplier for a certain good or material. Supply chain disruptions are not new. Industries know they have to prepare for the unexpected—earthquakes, droughts, extreme weather—and typically markets will normalize relatively fast.[43] The pandemic, however, posed a far greater challenge. While a natural disaster might hit one or two industries particularly hard, the pandemic impacted the economy at large, causing lasting shortages in a multitude of sectors.

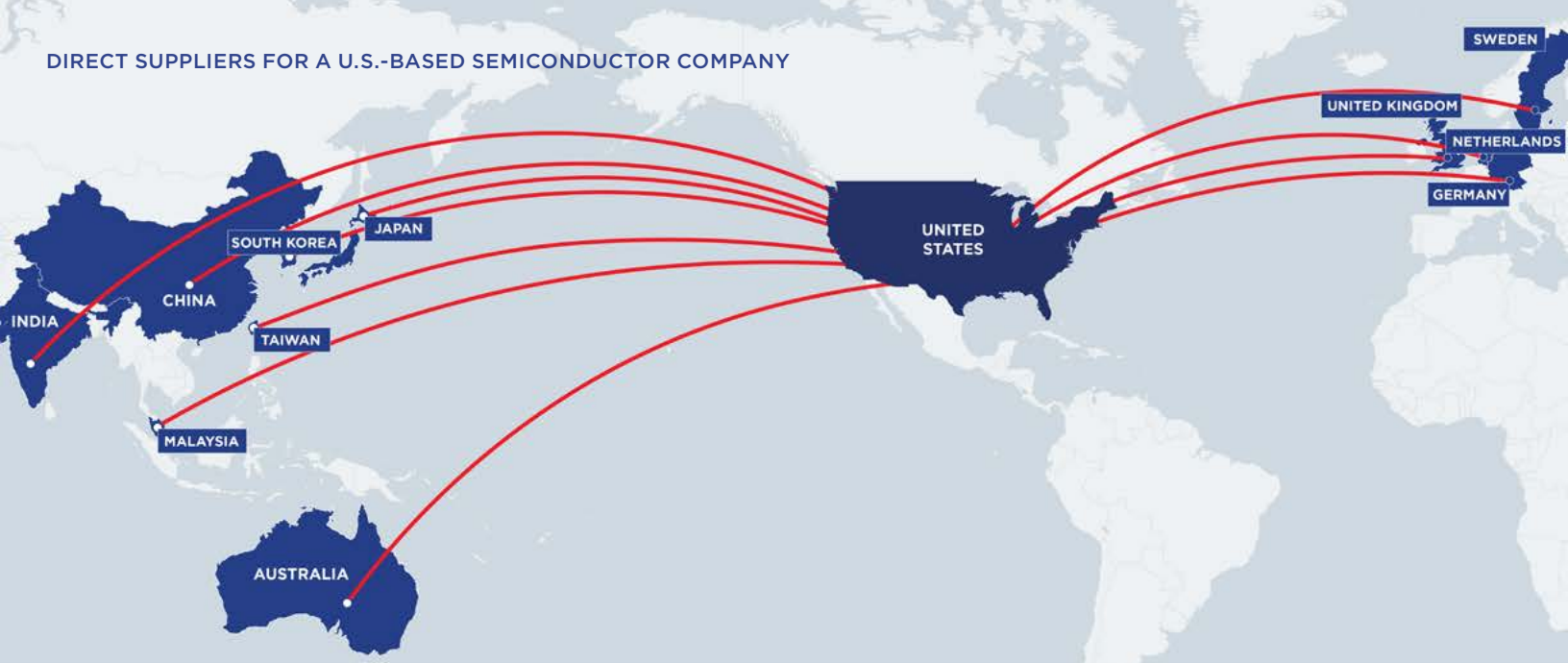
Many products today require materials from an assortment of manufacturers from across the globe. Certain materials may be available only in a specific region or through a limited number of suppliers—a kind of dependence that creates a higher risk of disruption for firms. Shortages in the healthcare industry were of particular concern in the early days of the pandemic. China—a major exporter of protective medical gear—paused much of its exports of surgical masks, diverting them to local hospitals instead.[44] Demand for N-95 masks was so high in the United States that government leaders asked the public to reserve the limited supply for frontline healthcare workers.

As factories shut down in early 2020, U.S. government officials were concerned about possible shortages in a variety of commonly used antibiotics and painkillers.[45] According to some estimates, about 80 percent of the active pharmaceutical ingredients (APIs) used in U.S. drugs are processed in China and India.[46] While major drug shortages did not materialize, the United States' dependence on foreign suppliers for critical pharmaceutical products revealed a glaring vulnerability.

Limited vendor diversity is not just an issue that arises between the United States and its competitors. Vendor diversity also can pose a problem among the United States and its allies. The telecommunications industry, for instance, is a highly consolidated industry with steep barriers to entry—which limits vendor choice and further complicates the global race in 5G wireless.

The Biden administration has focused on tackling supply chain vulnerabilities in its first year, particularly

DIRECT SUPPLIERS FOR A U.S.-BASED SEMICONDUCTOR COMPANY



UNITED STATES

- CLOUD COMPUTING
- COMPUTATIONAL SOFTWARE DESIGN
- DIGITAL PROCESSING DESIGN
- INTEGRATED CIRCUIT TESTING/ MANUFACTURING
- ENVIRONMENTAL REMEDIATION
- COMMERCIAL DATA/ ANALYTICS SERVICES
- ENGINEERING SOLUTIONS
- SEMICONDUCTOR WIRE/METAL MANUFACTURING
- SCIENTIFIC RESEARCH SOLUTIONS
- SYSTEMS & INFORMATION DESIGN
- SEMICONDUCTOR MANUFACTURING & TESTING
- ELECTRONIC COMPONENTS
- SOFTWARE & PROGRAMMING

SOUTH KOREA

- ELECTRONIC COMPONENTS
- SEMICONDUCTOR CLEANING/COATING
- SEMICONDUCTOR WIRE/METAL MANUFACTURING
- LIGHT-EMITTING DIODE TESTING

JAPAN

- ELECTRONIC COMPONENTS
- SEMICONDUCTOR MOLDING
- SEMICONDUCTOR MANUFACTURING & TESTING
- INTEGRATED CIRCUIT TESTING/ MANUFACTURING

TAIWAN

- ELECTRONIC CALCULATOR SOLUTIONS
- INTEGRATED CIRCUIT TESTING/ MANUFACTURING
- LOGIC NON-VOLATILE MEMORY DEVELOPMENT
- SEMICONDUCTOR MANUFACTURING & TESTING

CHINA

- SEMICONDUCTOR MANUFACTURING & TESTING
- SOFTWARE & PROGRAMMING

UNITED KINGDOM

- SEMICONDUCTOR MANUFACTURING & TESTING
- ELECTRONICS DESIGN SOFTWARE

GERMANY

- SYSTEMS & INFORMATION DESIGN
- CHEMICALS
- ELECTRONIC COMPONENTS

NETHERLANDS

- SEMICONDUCTOR MANUFACTURING & TESTING

SWEDEN

- INDUSTRIAL TOOLS/EQUIPMENT MANUFACTURING

MALAYSIA

- INTEGRATED CIRCUIT TESTING/ MANUFACTURING

AUSTRALIA

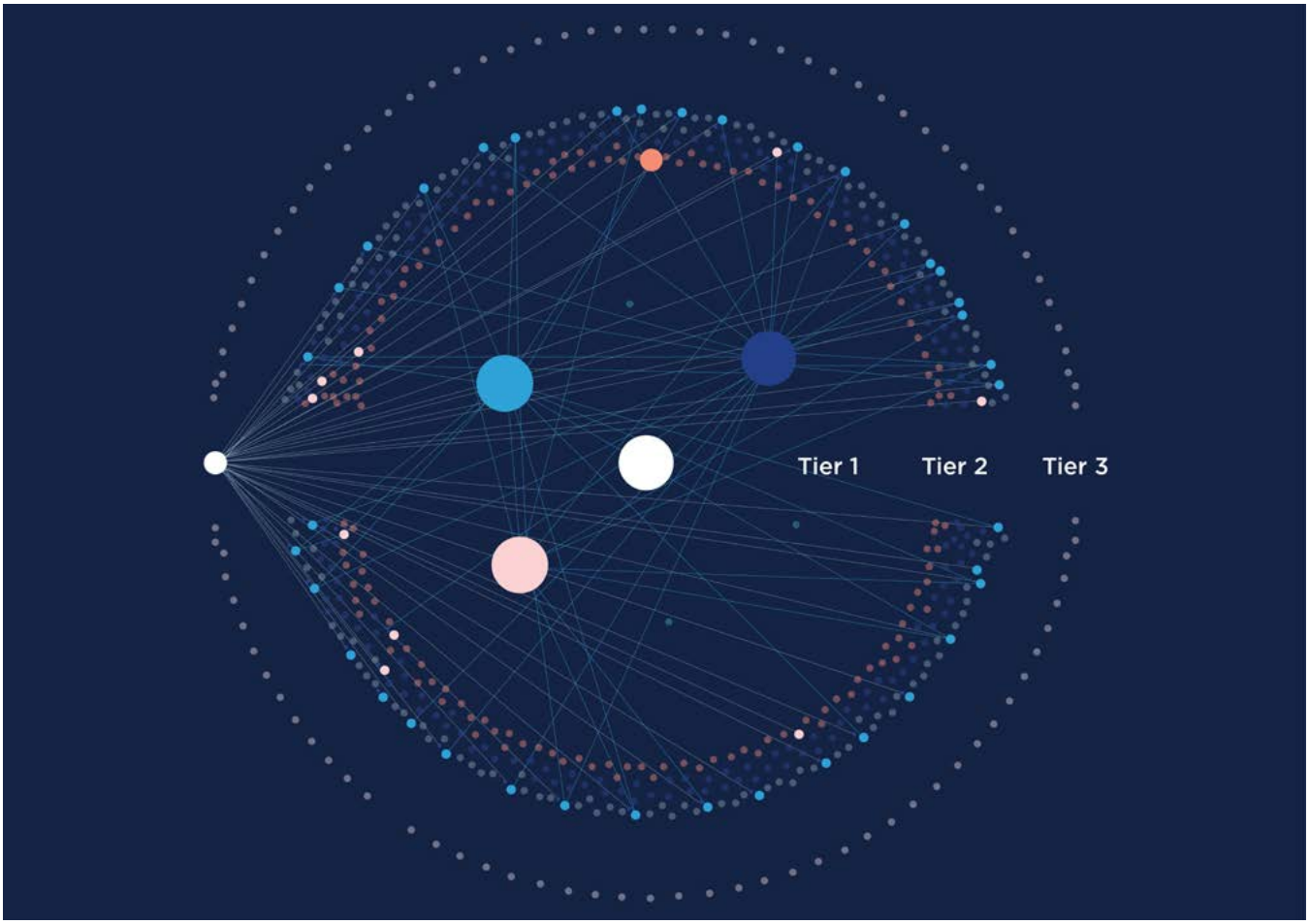
- SOFTWARE & PROGRAMMING

INDIA

- STATISTICAL ANALYTICS SOFTWARE

There are a multitude of diverse industries that serve as direct suppliers for a semiconductor company based in the United States. The graphic also shows the geographic concentration of certain industries within the semiconductor supply chain. (Data and graphic provided by Govini.)

SUPPLY CHAIN MAPPING AND RISK MANAGEMENT



Companies use interactive visualizations, like the example shown here, to help identify bottlenecks and potential supplier concentration risks in their extended supply chains. There are numerous firms that offer tools and expertise to support companies' desire to better understand their supply chain vulnerabilities. (Data and graphic provided by Interos.)

in industries facing shortages and with a higher degree of dependence on foreign suppliers.[47] In June 2021, the administration released a report with assessments on four critical products—semiconductor manufacturing and advanced packaging, large capacity batteries, critical minerals and materials, and APIs—and found that across these products, "insufficient U.S. manufacturing capacity" and "geographic concentration in global sourcing" were key risks that contributed to vulnerabilities in their supply chains.[48]

Some manufacturing firms have implemented new strategies to try to diversify their supply base. As the trade war between the United States and China intensified in recent years, some companies adopted a "China+1" strategy, meaning they attempted to expand production outside of China to an additional Southeast Asian country, such as Vietnam, Malaysia, Thailand, or Indonesia.[49] This strategy is meant to allow for greater vendor diversity—and to protect firms from an overreliance on China.

Limited Transparency

It can be difficult for industries to understand the full scope of their supply chain or take corrective actions to effectively remedy disruptions. Many supply chains are complex and diffuse, which makes meaningful transparency and effective contingency plans particularly difficult. For example, at the start of the COVID-19 pandemic, the world's 1,000 largest companies and their suppliers owned more than 12,000 facilities in regions affected by quarantine restrictions.[50] Efforts to uncover the pieces of their supply chain affected by the pandemic significantly affected production times. The need for supply chain transparency has never been greater.

According to Alexis Bateman, a research scientist at MIT, supply chain transparency "requires companies to know what is happening upstream in the supply chain and to communicate this knowledge both internally and externally."[51] This process is easier said than done. But as the difficulty of transparency increased over time, so too did its importance.

Many consumers are demanding a greater degree of transparency. Some are seeking it in response to lasting shortages throughout the pandemic. A study from Oracle found that Americans are increasingly concerned about lasting delays, product shortages, and widespread disruption to supply chains.[52] A sizable portion of respondents wanted greater transparency on inventory (59 percent) and potential supply chain issues (54 percent).[53] A growing number of consumers also desire transparency because they want to know how their merchandise is made and where it comes from.[54] Research from MIT Sloan School of Management found that consumers value information on how workers are treated, and may be willing to pay more for products from companies with greater supply chain transparency.[55]

There is also growing interest in laws and government regulations on supply chain transparency. Earlier this year, for instance, the United States banned imports of cotton from the Xinjiang region of China over human rights abuses against the Uighur population, affecting a variety of U.S. retailers.[56] The blacklisting included 87 percent of China's cotton crop, or one-fifth of the world's total supply.[57] Before the ban took hold, the Workers Rights Consortium estimated that U.S. retailers imported more than 1.5 billion garments containing materials from Xinjiang per year—more than $20 billion in retail sales.[58]

Another example of required supply chain transparency is government regulations on food safety. In 2011, Congress passed the Food and Drug Administration (FDA) Food Safety Modernization Act (FSMA)—the first major overhaul in the country's food safety system since 1938.[59] The FSMA was designed to shift America's food safety system from responding to foodborne illnesses to preventing them altogether.[60] The then-Deputy Commissioner of the FDA Michael Taylor described the FSMA as "supply chain management written into law."[61] Ten years later, the FSMA has led to the creation of new rules and authorities intended to better regulate the production and transport of food produced domestically and imported.[62]

Despite moves by governments, companies, and consumers to promote greater supply chain transparency, achieving meaningful transparency is a difficult task. This is particularly true for supply chains with multiple tiers of suppliers, and due to complex laws regulating contractual responsibility. For one, supply chains are not necessarily designed for transparency.[63] Today's manufacturing models often prioritize efficiency and cost reduction over resiliency, security, and transparency. For some companies or industries, the necessary data and information for meaningful transparency may not be easily collectible or accessible.[64] Finally, some companies may be reluctant to share certain information about their supply chains out of fear that it could make them vulnerable to criticism or disadvantage them in a competitive market.[65] As White House economic advisors Helper and Soltas explain, when it comes to automakers and semiconductor manufacturers, neither "can trace what goes in these intermediate layers (or "tiers") of the supply chain, due in part to lack of trust among parties in supply chains, who fear the information might be used to replace them or to bargain for a price reduction."[66]

Many supply chains are complex and diffuse, which makes meaningful transparency and effective contingency plans particularly difficult.

Ultimately, greater supply chain transparency results in far more advantages than disadvantages. As the events of the past two years have shown, industries must be prepared for unknown fragilities in their supply chains caused by any number of events—pandemics, blocked canals, natural disasters, cyberattacks. Transparent supply chains are, in turn, more resilient and secure.

Each of these vulnerabilities introduces fragility into the system of global supply chains. There is no question that supply chains are not adequately resilient to handle mass disruption, particularly disruption so widespread and long-lasting. To address these and other vulnerabilities, the U.S. government must create a new paradigm to secure and strengthen critical supply chains.

A Supply Chain Remapping Schema

The United States requires a framework to inform a new conceptual approach to supply chain resilience. The goals and objectives of this approach are to be tied directly to the United States' national security and economic security goals, and its technology and industrial policy strategies. Stakeholders in industry should play a key role in planning and executing this framework.

The Question of Necessity

To articulate an executable strategy, U.S. policymakers must first categorize supply chain considerations by priority. Each of the three categories will require different policies to plan, initiate, and sustain an enduring supply chain strategy.

ESSENTIAL

This category comprises outputs deemed essential for the day-to-day functioning of American society. While the United States should strive for complete self-sufficiency where possible, the minimum goal should be to ensure domestic capacity to produce 80 percent of regular daily needs during a multiyear crisis. Given the cost and related inefficiencies of autarky, the list of what qualifies should be short. Examples of plausible candidates include pharmaceuticals and medical equipment. Creating and maintaining secure and resilient supply chains for essential inputs and products will require government-led industrial policy on a scope and scale not seen in decades.

STRATEGIC

Most inputs and products key to U.S. national and economic security will fall in this category. Self-sufficiency is likely to be infeasible or prohibitively expensive because the United States doesn't have all the requisite technologies, capabilities, and know-how. At the same time, the United States should have minimal to no dependence on strategic rivals and potential adversaries, requiring supply chain strategies to be developed through bilateral and multilateral arrangements with trusted partner countries. Critical minerals and semiconductors are sectors that would be included in this category. Creating and maintaining secure and resilient supply chains for strategic inputs and productions will require significant government engagement with the American private sector and partnerships with foreign governments and companies.

NON-ESSENTIAL

Most items that fuel the American consumer economy are not essential to the country's day-to-day needs. Many are also fungible—they can be replaced with similar items having the same function. Nevertheless, there is substantial economic activity at stake when supply chain disruptions occur. Examples of items in this category include consumer goods such as apparel, furniture, and building materials. Introducing greater resilience in supply chains for non-essential items should mainly be the purview of industry reacting to market forces.

The Question of Geography

Once priorities are set, leaders in government and industry alike must consider "where to?" when looking at remapping supply chains. The geographic component of a new supply chain strategy has four components. The first component is **homeshoring.** The United States has much to gain from greater production and manufacturing at home, particularly in high-end technologies. Unsurprisingly, the concepts of onshoring and reshoring—bringing new capacity to the United States and bringing old capacity back, respectively—have great appeal to politicians. With the exceptions of outputs classified as "essential," however, U.S. policymakers should recognize that external dependencies will remain. Managed well, those dependencies can be turned into assets through enhanced alliances and partnerships with key countries.

To do so, the concept of **friendshoring** holds promise. Here the goal is to ensure that strategic supply chains are based in allied and highly trusted partner countries and have minimal to no reliance on inputs from potential adversarial countries. At its most cohesive, a friendshoring arrangement could culminate in a technology alliance, such as for semiconductors. In such a scenario, Australia, Canada, the EU, India, Israel, Japan, South Korea, Taiwan, the United Kingdom, and the United States could agree to create a complete and geographically diversified supply chain.

A related concept is **nearshoring**, where the production and manufacturing is closer to home in a neighboring or nearby country. For the United States and allied countries, such a strategy is often synonymous with friendshoring.

The fourth concept is **regionalization.** The goal here is to have production capacity in various parts of the world to meet regional demand. Although this concept is mainly of interest to business leaders concerned with non-essential mass market products such as apparel, there is potential utility for national security–related concerns. The U.S. Department of Defense could work with defense contractors, for example, to set up small forward-deployed manufacturing hubs at major U.S. military installations to ensure quick-turn availability of components.

Critical minerals are a strategic raw material for many of America's most important supply chains. Reliable access to minerals such as iron ore (pictured here) allows the United States to fuel its domestic manufacturing capabilities. (Anton Petrus/Getty Images)

A New American Industrial Policy

The United States needs a new industrial policy as part of a broader strategy to secure national needs. America's innovative private sector is one of its great strengths, and American companies have achieved long-standing successes. Over the past three decades, U.S. policymakers have stood mostly on the sidelines as the private sector molded the American economy and developed a highly globalized system. This system worked well during the Cold War, when America's chief adversary was economically feeble, ill-equipped to benefit from the global economic system, and largely untethered from U.S. economic activity.

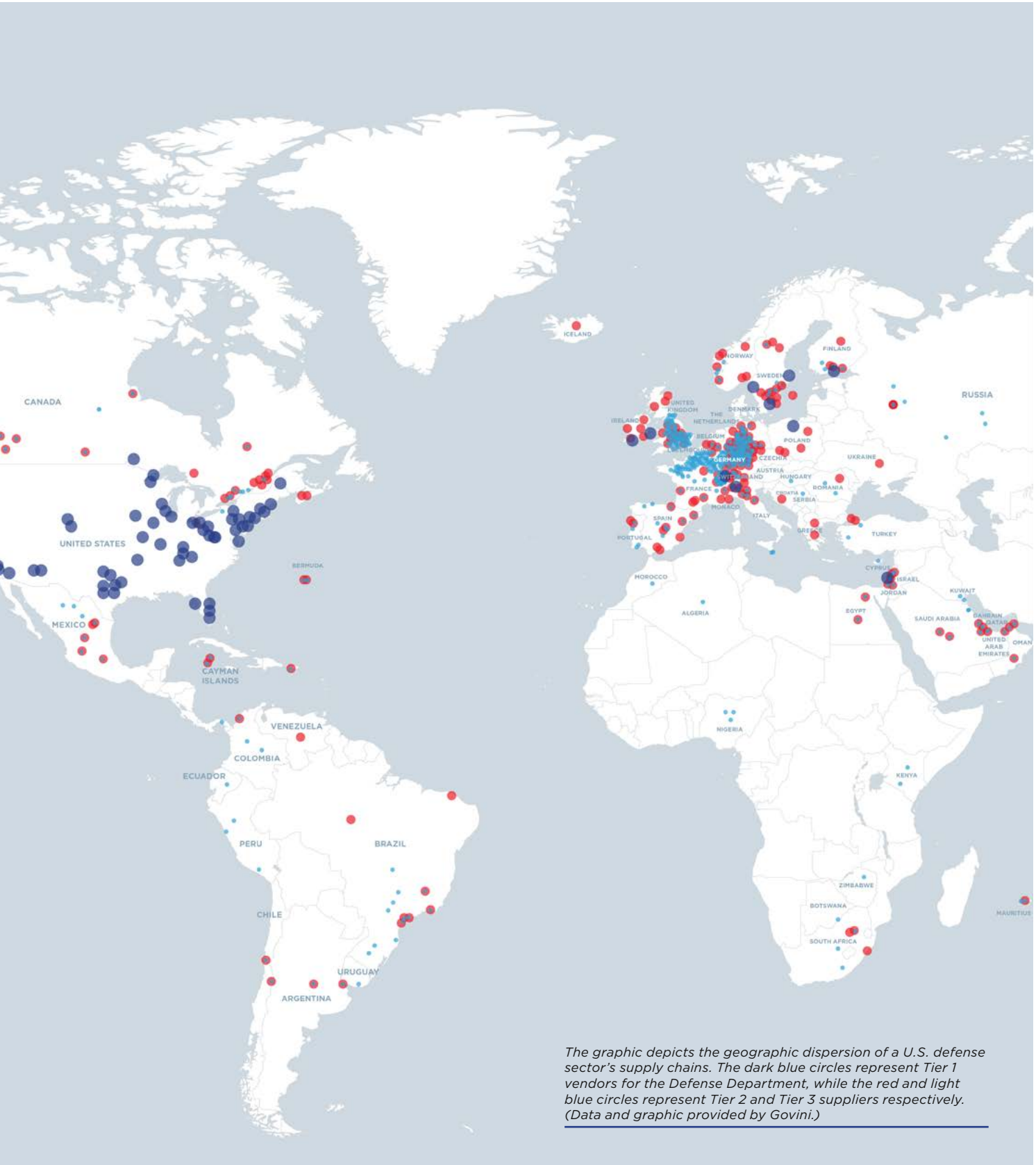
The rise of China as an economic, technological, and military powerhouse, however, has eroded many of the upsides of that globalized system, and the resulting imbalance is increasingly problematic for the United States and its allies. The United States is highly dependent on China for key inputs such as rare earth magnets and critical minerals. Shortages of basic goods such as pharmaceuticals and medical equipment throughout 2020 underscored the risk in achieving economies of scale through geographic concentration.[67] Similarly, in late 2021, curbs on magnesium production in China, which has a near total lock on global supply, threatened major shortages in aluminum production that could cripple the global automotive industry.[68]

Righting the ship will require policymakers to acknowledge that a new approach is needed in response to this geopolitical reality. The U.S. government must change how it engages with industry, from incentives to regulations, and re-up its historical role as a driver of technological development through increased investments in research and development (R&D), especially early-stage research that companies tend to avoid.

Specifically for supply chains, step one is for U.S. government officials—particularly experts from the departments of Defense, Commerce, State, Health and Human Services, and Energy; the intelligence community; and the national labs—to determine the supply chains where vulnerabilities pose an unacceptable risk to U.S. economic and national security. President Joe Biden's Executive Order on America's Supply Chains is an important starting point.[69] These assessments must be made permanent and continuous, which would be most effectively achieved by bolstering the Department of Commerce with expanded authorities and more resources.

SUPPLY CHAINS MAP FOR A U.S. DEFENSE MARKET SECTOR, TIERS 1–3*

* Only foreign suppliers shown for Tiers 2 and 3



The graphic depicts the geographic dispersion of a U.S. defense sector's supply chains. The dark blue circles represent Tier 1 vendors for the Defense Department, while the red and light blue circles represent Tier 2 and Tier 3 suppliers respectively. (Data and graphic provided by Govini.)

As the supply chains considered to be essential are identified, step two is for U.S. government officials to work with industry to map and audit those key supply chains and identify knowledge gaps. Numerous firms offer tools and expertise that can support such work. Industry should welcome this effort, but Congress should be prepared to act should cooperation prove wanting.

Third is crafting a strategic plan to disentangle and diversify those supply chains. Doing so well will require a government-led effort centered on close collaboration with and incentives for industry stakeholders and, in most cases, with allied and partner governments and their private sectors. Here also, the Department of Commerce will play a major role as will the Department of State, which will need to build up techno-diplomatic capabilities.

Modern day supply chains rely on complex and congested port systems to transport raw materials and finished goods between their destinations. Here, a security guard monitors the operations of a U.S.-based port from the control room. (Jon Feingersh Photography Inc/Getty Images)

Supply Chain Effectiveness

The dominant measure of a supply chain's success must shift from efficiency and optimization, where the driving factors are speed and lowest-possible costs, to one of effectiveness, which prioritizes security, robustness, and resilience. Effective supply chains are ones that eliminate single points of failure wherever possible, feature geographic and vendor diversity, and incorporate surge capacity. In essence, this is the "selective decoupling" that many policymakers and pundits are clamoring for: a combination of reshoring and remapping of key supply chains to enhance economic security and reduce reliance on China in particular.

Achieving this will be difficult and expensive. Executing it well will require careful planning and coordination by government and industry leaders. Congress will have to commit to funding and providing incentives for infrastructure development such as ports, railways, highways, and energy, as well as tax breaks for relocating manufacturing facilities.

Strategic Interdependence

Remapping global supply chains will require the United States to collaborate with allies and partners. American self-sufficiency in most areas would be unaffordable and, in many cases, unachievable. Rather than pursuing wholesale onshoring and reshoring efforts, U.S. leaders should plan instead for solutions with the premise of strategic interdependence, where two or more countries work together to meet a common goal. The Biden administration is setting out to do just this—using the "friendshoring" term—bilaterally with Japan and South Korea, and with multiple countries through, for example, the Quadrilateral Security Dialogue and the U.S.-EU Trade and Technology Council.[70] Similarly, officials during the Trump administration initiated a fledgling Supply Chain Resilience Initiative, although that effort did not endure. Other logical countries for comprehensive supply chain agreements include Taiwan and Singapore.

A Closer Look: Supply Chain Case Studies

Resolving America's critical supply chain issues is particularly challenging because each sector's supply chain contains unique features—due to multiple layers and suppliers—and therefore varying vulnerabilities. Many of the underlying challenges, however, are consistent, and a deeper analysis can offer valuable lessons moving forward.

This section explores the semiconductor supply chain and software supply chain. While vastly different in their end product and sources of fragility, they share many of the same vulnerabilities, such as limited transparency and brittleness. Understanding the risks and vulnerabilities of these specific supply chains highlights not only how vast the challenge of supply chain security is, but how important it is to U.S. national security and economic prosperity.

The Semiconductor Supply Chain

One of the more pressing supply chain vulnerabilities the United States faces relates to semiconductors. These tiny components provide the computational horsepower needed in almost every single electronic device used today. Semiconductor chips are found in a variety of machines, ranging from simple appliances like coffee makers and alarm clocks, to state-of-the-art military technologies and quantum computers. Over the past three decades, the volume of semiconductors in devices has continued to rapidly accelerate. While this acceleration has improved device capabilities, it also dramatically increased the chip density in devices and demand for more chips.[71]

Securing the semiconductor supply chain remains an ongoing national security challenge for the United States. This critical supply chain serves a vital role in the U.S. national security apparatus by enabling the development of key technologies and capabilities, not to mention sustaining the consumer economy. Without a reliable supply of industry-leading semiconductors, private manufacturers in the United States and allied countries will be unable to develop, test, and produce their increasingly high-tech products and meet growing customer demand.

Emerging fields such as quantum computing applications are especially struggling to continue advanced research due to the current shortages of semiconductors, and the situation does not appear to be improving soon.[72] Exacerbated by the pandemic, the consequences of a brittle semiconductor supply chain are now readily clear and will require swift action from policymakers to secure it.

Vulnerabilities throughout the semiconductor supply chain can be divided broadly into two groups. First is the geographic disparity between centers of design for processors and where they are ultimately manufactured. Second is a lack of transparency, as well as elastic demand signals. Although these weaknesses are especially crippling to the semiconductor supply chain, they are not particularly unique nor insurmountable obstacles. Restructuring this supply chain is a critical national security objective that will shape the course of American economic and military superiority in the years to come.

In the early development stages of semiconductors in the 1960s, the United States established itself as the global leader in development and design of advanced semiconductor chips. Much of this was due to early public investment throughout the 20th century that enabled innovative approaches and a culture of information sharing among manufacturers. Throughout the Cold War, American industry partnered with the military to design and mass-produce these chips—a necessary step to propel the booming space and missile industry.[73]

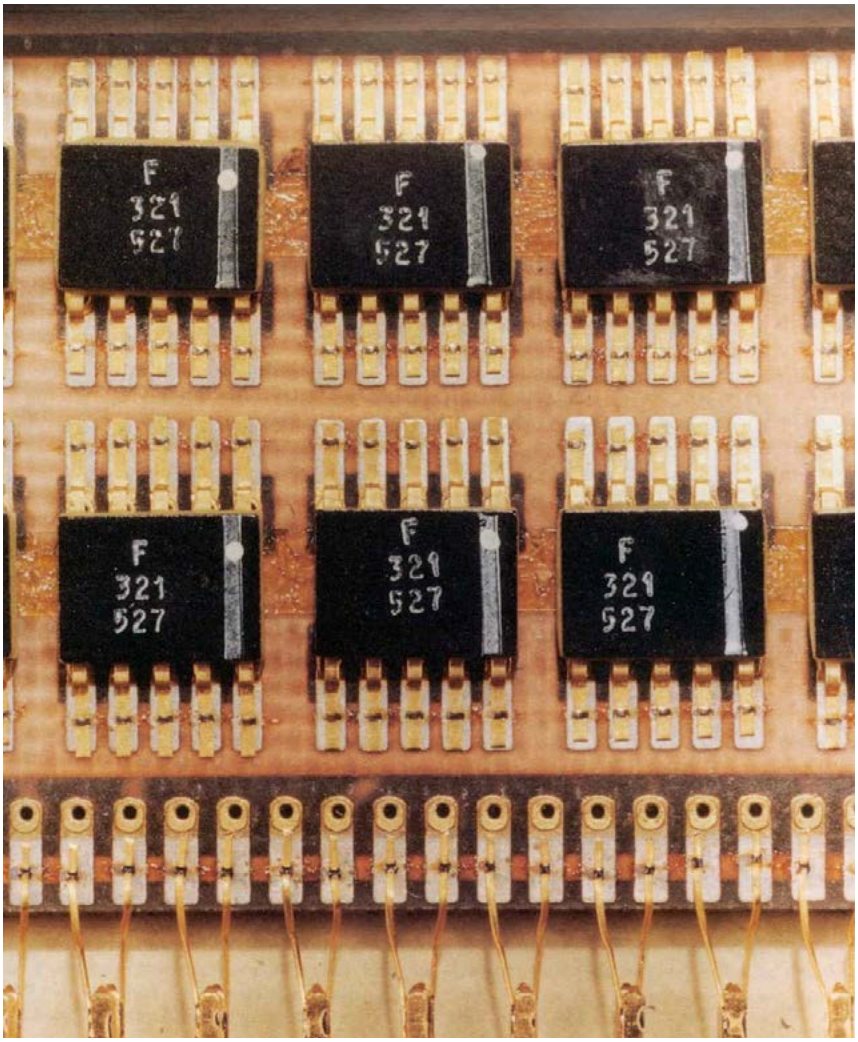
Despite its first-mover advantage, American semiconductor design preeminence did not last forever. Reductions in government R&D and extensive investment by the Japanese government in design and manufacturing capacities shrank U.S. market share from 85 percent to an estimated 20 percent by 1993.[74]

In response, the U.S. government intervened once again by partnering with the newly formed SEMATECH (Semiconductor Manufacturing Technology) in 1987. This consortium of 14 U.S.-based semiconductor firms sought to incentivize cooperation among American firms and overcome the stifling lack of consensus among domestic competitors regarding trade restrictions toward Japan.[75] As a result of this cooperation among U.S. producers and policymakers, chip design costs dropped significantly within the United States, and new, innovative chips were able to be designed domestically.[76]

Although America still maintains its design advantage today, China and other near-peer competitors are working tirelessly to catch up. Increased R&D investment in semiconductors and other critical technologies indicates the Chinese Communist Party recognizes the importance of surpassing the United States in this area of competition. Over the past 25 years, China's rate of investment in R&D as a percentage of GDP has caught up to that of the United States, and is now just 0.7 percentage points behind.[77] While America's semiconductors are still about two generations ahead of those designed in China, China's are rapidly catching up.[78] As Robert Work, former deputy secretary of defense and co-chair of the National Security

Commission on Artificial Intelligence, points out, the United States is only 110 miles away from losing its competitive advantage entirely. "If China absorbed Taiwan—which is the source of much of the world's hardware—that would really be a competitive problem for us."[79]

But design plans only matter if the actual chips can be manufactured and distributed. While U.S. industry retains the lead in designing semiconductors—an advantage it must prioritize maintaining—it lacks the ability to manufacture these processors domestically, or within reliable, secure, and resilient supply chains. A report on the current state of semiconductors published by the SIA finds that in 1990, the United States held 37 percent of the world's semiconductor manufacturing capabilities. Today that number is less than 12 percent and is continually dropping.[80] Conversely, today over 70 percent of semiconductors are manufactured in Asia, with Taiwan and South Korea holding the vast share of that percentage.[81]



America's early lead in the semiconductor sector was due primarily to massive government investment in space technologies and the creation of the National Aeronautics and Space Administration. An integrated circuit like the one pictured here was used on the Apollo spacecraft that eventually took the first humans to the moon. (Henristosch/Wikimedia)

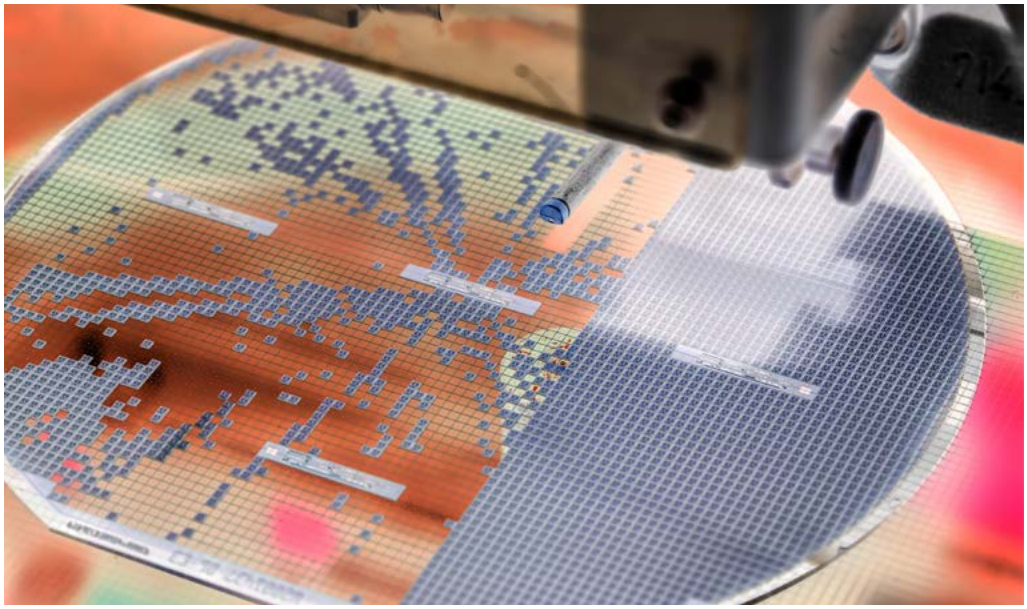
A primary cause for the United States' dwindling manufacturing capabilities is misalignment of interests and lack of government involvement. Because of the complexity of manufacturing these processors, building semiconductor fabrication sites, or fabs, requires significant investment and capital, which private industry is naturally hesitant to make. New, significant federal investments in domestic semiconductor manufacturing would be projected to add billions to the U.S. economy and create thousands of new jobs.[82] Intel, an American semiconductor giant, recently announced its plans to build two semiconductor fabs worth $20 billion in Ohio.[83] Moves such as these signal the growing recognition among policymakers and industry leaders that domestic semiconductor manufacturing capabilities are strategically critical.

Looking at leading manufacturing countries, it is clear that government investment is the common catalyst for semiconductor production. Taiwan's preeminent Taiwan Semiconductor Manufacturing Company (TSMC) accounts for 50 percent of the global market of semiconductors. It registered $115 billion in annual revenue through 2020 and surpassed projection by increasing revenue by 25.9 percent in 2021.[84]

Taiwan's rise in semiconductor manufacturing capabilities began in the 1970s when the government identified chip manufacturing as one of its key future industries. At the time, Taiwan's economy relied primarily on agricultural products and therefore lacked the domestic production infrastructure needed to meet the government's semiconductor goals.[85] As in the United States today, private industry also lacked the capital and incentives needed to invest of its own volition. Recognizing this gap, the Taiwanese government created the country's first semiconductor fab in 1975, purchasing the designs from RCA—a

leading American tech giant at the time.[86] When private investment was still noticeably lacking, in 1987 the government established another chip manufacturer, TSMC, but with the condition it would only hold 50 percent of the company's share. Partnering with Philips Electronics, which took 35 percent of the other share in the company, this policy abated much of the risk that disincentivized private companies from initially investing.[87]

In the following decades, concurrent with explosive global demand for chips, government funding slowly tapered as private sector companies realized the profitability of Taiwan's booming manufacturing capabilities. Throughout the 1990s, TSMC was able to make its own successive investments to match growing demand, including an $800 million fab site in 1994 and a $1.2 billion facility in 1995.[88] While government investment continued throughout the entire semiconductor ecosystem, today it has largely transitioned to R&D as opposed to manufacturing-specific capabilities. For example, this past year Taiwan announced it would invest $300 million in advanced degree programs in order to safeguard the country's innovative edge and talent base.[89] Taiwan's semiconductor history makes it clear that government investment is not a sinkhole, but rather a catapult. Semiconductor manufacturing is resource and labor intensive, meaning private investors are unlikely to spur capabilities without incentives. If the United States wishes to recapture its production capabilities, at first it will take the government footing the bill upfront.



Today, the Taiwan Semiconductor Manufacturing Company (TSMC) is the leading chip manufacturer in the world. The company's ability to quickly improve its capabilities is a result of early government investment in production capabilities. (MACRO PHOTO/Getty Images)

The second vulnerability affecting the semiconductor supply chain is a lack of transparency and consistent demand signals. Without both of these components, vendors cannot supply chips reliably in a timely manner. Instead, the demand for semiconductors regularly fluctuates and leads to surges and stalls in semiconductor production. Bubbles and shortages further exacerbate the issue and signal the need for more consistent and strategic leadership in managing the semiconductor supply chain.

Well before the pandemic, the resilience of America's semiconductor supply chain was fragile underneath its veneer of stability. Chip manufacturers lacked key features necessary to bounce back from shortages and blockages, such as diversified suppliers of rare earth metals and responsible demand levels from industry, especially car manufacturers. Experts recently have described the semiconductor supply chain as having a "bullwhip" effect, like some commodities.[90] Even small movements of the hand cause the whip to move dramatically; likewise, small fluctuations in demand for semiconductors lead to outsized production changes.

Like every other critical supply chain, the global shutdowns disrupted demand for many products that used semiconductors as well as hindered manufacturing. Automakers were particularly affected by COVID-19, experiencing a dramatic decline in vehicle sales during the first few months of the pandemic. In response, manufacturers slashed their orders for all the parts and materials needed to manufacture their cars, including the processors used in touch screens and smart sensors surrounding the vehicle.

In response, the semiconductor industry likewise slashed its production of car-specific chips. Because of the brittle supply chain, however, even nearly two years later there are still considerable delays for the production of new cars (paired with increasing density of chips needed per car). As of January 4, 2022, the average lead time for a semiconductor is 25.8 weeks—an excessive lag for such a vital piece of technology.[91]

As the globe continues to wrestle with the ongoing pandemic, demand for semiconductors does not show any signs of dissipating. As shortages continue, a few important lessons can be learned and policies implemented. The first is that government intervention is needed to spur manufacturing capabilities domestically. Should the United States keep its competitive edge against China and other emerging technology competitors, it cannot rely on private industry alone to take charge. Instead, policymakers must be ready to engage. The bipartisan CHIPS for America Act, introduced in February 2021, is a step in the right direction and signals recognition within Washington of what needs to be done.[92]

Policymakers also must recognize the geostrategic implications of these critical technology supply chains. The ubiquity of semiconductors and other essential technological components are necessary to propel innovation in seemingly disparate industries. As societies continue to rely on these chips, they become more and more essential. A potential consequence of this dynamic is that states will pursue increasingly protectionist economic policies to safeguard their access to chips, or will make their manufacturing capabilities indispensable. A disruption to America's semiconductor supply chain either could instigate, or be a consequence of, geopolitical rivalry between the United States and adversarial nations.

The demand for semiconductors regularly fluctuates and leads to surges and stalls in production. Bubbles and shortages further exacerbate the issue and signal the need for more consistent and strategic leadership in managing the semiconductor supply chain.

Finally, when competing with adversarial economies such as China, harmonization among domestic industries is essential. Semiconductors, AI, and other technology developments are predominantly driven by the private sector. As seen with the SEMATECH example, the United States lost its competitive advantage to Japan in the 1980s in part due to a lack of cooperation among American firms and a zero-sum mindset.[93] The United States must cultivate an environment for trust, transparency, and cooperation throughout the semiconductor supply chain to successfully counter adversarial nations with advanced and robust industrial bases in the future.

The Software Supply Chain

Much of the current debate surrounding supply chain security is focused on hardware, such as 5G base stations, next-generation silicon semiconductor chips, or medical equipment. But with the ongoing digital transformation in government and industry alike, software is playing a growing role. The software supply chain consists of the sequence of processes, goods, or services involved in the production and deployment of software systems. It includes everything that might go into the software—the codebases, dependencies, libraries, and other components.

Unlike traditional supply chains, software supply chains are unique in that the final product often requires continuous updates and patches. While this continuous revision of software allows trusted developers to fix potential cybersecurity issues as they materialize, it also provides an opening for hackers who might impersonate updates to corrupt the systems.

The security of software supply chains presents a unique and critical challenge for U.S. national security. According to the Atlantic Council's database of supply chain incidents, over 20 percent of the 138 cataloged supply chain cyberattacks were carried out by nation states between 2019 and 2020, including government-backed groups in China and Russia.[94] Cyber espionage efforts, which may go undetected for months on end, put America's critical infrastructure, security, and long-term competitiveness at risk.

Demand for software capabilities shows little sign of dissipating. The U.S. Department of Defense is on track to spend over $12 billion on information technology systems from 2019 through 2022.[95] These systems range from financial and human capital management databases to those that provide information to organize, monitor, or direct mission operations.[96] For the vast majority of these systems, the Defense Department uses a commercial off-the-shelf (COTS) procurement model. This allows government officials to buy or repurpose existing commercial software components as opposed to contracting a bespoke software for the government (referred to as the government off-the-shelf model). COTS is the dominant procurement model because it is significantly cheaper and easier to source commercial software, and government departments may not have the technical capacity needed to develop and deploy certain software systems.

As a result, COTS is used for almost every aspect of government software systems, from custom software for unmanned aerial vehicles to VPNs for remote work.[97]

In recent years, the software development industry increasingly has used open-source libraries, which allows anyone to access, modify, and distribute the software code. In fact, presently 99 percent of all codebases contain one component that is open source—an increase of over 259 percent in the past five years.[98] Open-source libraries save time and money by democratizing access to source code and increasing collaboration. For all its benefits, however, open-source ecosystems and libraries create many potential security vulnerabilities as well.

These vulnerabilities in existing software supply chains have led to significant cyber incidents. So-called supply chain cyberattacks, which have been used in some of the most notable incidents, such as the Kaseya and SolarWinds attacks, target vulnerabilities in software vendors or IT services to then compromise end users.[99] While the basic framework of a supply chain attack is to compromise suppliers at any location in the supply chain, there are many variations of such attacks. For example, attacks might include malicious insertion in software components, updates, or system data. Attacks also might happen at various points (e.g., software development locations, software support providers, prime or sub software contractors) and at various times (e.g., preacquisition/development, acquisition, or postdeployment).[100]

In the SolarWinds hack, for example, Russian state-affiliated hackers first infiltrated the network infrastructure of SolarWinds, a company that produced the remote network and application monitoring platform Orion. Attackers then were able to distribute compromised software updates to end users, which included many large corporations, all branches of the U.S. armed forces, and key federal agencies.[101] With these compromised targets, attackers were able to inject malware, compromise Microsoft's identity software to bypass multi-factor authentication, and gain access to nearly a dozen federal agencies.[102]

This campaign was unique in the compromise of key cloud-based systems, which enabled the initial breach to spread and allowed attackers to exfiltrate a significant amount of sensitive data. The SolarWinds hack and related supply chain attacks suggest several lessons for cybersecurity. On one hand, the ubiquity and usage of cloud services opens new vectors for potential attack. But on the other hand, existing approaches to software supply chain security by governments do not match the important new ways in which systems are built and deployed.

A more general lesson is the growing importance of engaging with trusted vendors and public-private coordination on cybersecurity. According to recent analyses of supply chain incidents, suppliers did not know or failed to report compromises in over 66 percent of attacks.[103] In most of these cyber incidents, attackers focused on suppliers' codes, necessitating a greater focus on continuously validating and monitoring third-party software by governments.[104]

Colonial Pipeline, a major U.S. oil pipeline operator, was the victim of a ransomware attack in May 2021. Pictured here is one of the company's hundreds of fuel-holding tanks located along the East Coast of the United States. The company preemptively shut down its 5,500 miles of pipeline for several days, causing disruptions to fuel supplies across the United States. (Drew Angerer/Getty Images)

While the federal government recently has acted—including an executive order that lays out new security requirements for commercial software—to address the risk of supply chain attacks, the vulnerability persists. In a recent survey of cybersecurity professionals, 84 percent see supply chain attacks being one of the most significant cybersecurity threats in the next three years. In 2021, the average ransom payment increased by 63 percent from the previous year, now $1.79 million.[105] These trends show the need for immediate action by the policymaking and cybersecurity communities to improve the resilience of software supply chains and take a more proactive approach.

These issues are not just cybersecurity challenges, but supply chain issues. This reality indicates a need to focus on sourcing practices and addressing vulnerabilities from foreign interference. The recent executive order on cybersecurity (E.O. 14028) is explicit in referring to "Software Supply Chain Security." The ongoing focus on software supply chain security and the preliminary National Institute of Standards and Technology guidelines (as ordered by E.O. 14028) indicate important steps in the right direction.

Although current Buy American Act provisions exempt COTS software and information technology, the Biden administration has signaled a willingness to review the current exemption but thus far has not taken substantive action.[106] Regardless of whether the exemption is lifted, the federal government has shown a greater interest in sourcing domestic software products due to cybersecurity concerns. But much more can be done to integrate software supply chain security with more comprehensive action to strengthen America's critical supply chains.

Despite recent cyber incidents demonstrating the vulnerability of America's software supply chains, existing supply chain security efforts do not explicitly mention software supply chains. While there has been a 100-day supply chain review of semiconductors, no such review is planned for IT and software. By 2022, a supply chain review of the information and communications technology industrial base is expected (pursuant to E.O. 14017). This should include a review of software supply chains, and potential vulnerabilities that come with critical software. Legislative proposals, such as the amendments developed by the House Armed Services Committee's Defense Critical Supply Chain Task Force for the next National Defense Authorization Act (NDAA), also should include software supply chain mapping, evaluations of foreign software dependence, potential vulnerabilities with commercial vendors, and opportunities to work with like-minded allies and partners.[107]

Finally, there is an opportunity to invest in new technologies and approaches for software supply chain security. AI tools could improve cybersecurity and augment the detection of potential threats.[108] Open-source cryptography systems—like in-toto, a project developed by New York University Center for Cybersecurity researchers and funded by the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA)—can strengthen software supply chain integrity by ensuring each step of software development proceeds according to specific protocols.[109] Additional R&D, in collaboration with academia and industry, can develop innovative responses to future software supply chain attacks.

Recommendations to Promote Supply Chain Resilience and Security

Building resilient, secure, and transparent supply chains will be a long-term, iterative challenge with input and involvement needed from the White House, Congress, a slew of government agencies, and private industry. Strengthening supply chains, particularly those critical to U.S. defense and economic prosperity, also will require persistent collaboration with allies and partners. This section offers recommendations for meaningful steps the U.S. government can take to secure its supply chains. Some of these actions can be taken in the short term, while others will require investment and attention for years to come.

The recommendations are split into two categories. The first category, "Manage Supply Chains," explores how the U.S. government can create and implement policies to monitor, assess, and remap certain supply chains. It also provides recommendations for how the U.S. government can better prepare for future supply chain disruptions and upheavals surrounding security and resiliency, as well as strategies for remapping certain supply chains. The second category, "Transform Supply Chains," includes recommendations for institutional changes in government, improving supply chain management with new technologies, and avenues for restructuring supply chains with allies and partners. Taken together, these recommendations contribute to an overarching strategy to ensure U.S. supply chain resiliency and security.

Manage Supply Chains

The U.S. government should craft and implement policies to strengthen and secure supply chains. The COVID-19 pandemic revealed vulnerabilities in America's current supply chains, and policymakers have an important opportunity to ensure that U.S. supply chains are more resilient.

To that end, the White House, with the support of Congress, should:

Craft a supply chain strategy. The United States needs a blueprint for how to think about, and prioritize, the security and resilience of its critical supply chains. Undergirding any strategy must be the understanding that some supply chains can be reasonably restructured while others cannot. Policymakers must determine which supply chains are "essential," meaning the United States strives for self-sufficiency; supply chains that could be deemed "strategic," where the United States focuses on eliminating the influence of adversarial competitors through greater domestic capacity and through strategic interdependencies with allies; and "non-essential" supply chains where industry can focus on market forces to determine the most desirable configuration. Other elements of a strategy should include investments in supply chain resilience, robust reporting for supply chain transparency, international collaboration, and partnering with private industry.

Remap critical supply chains. Many supply chains important to U.S. economic security and national defense are dangerously brittle. Addressing these vulnerabilities will be expensive, complex, and time consuming. The risks of not restructuring these supply chains, however, are even greater. First, policymakers and government officials must identify supply chains with vulnerabilities that pose an unacceptable risk to U.S. national security and economic security. Policymakers, in conjunction with industry leaders, must audit these essential supply chains. Finally, policymakers will need to craft a roadmap for how to successfully disentangle the critical supply chain. Geography, natural disasters, and climate change also must be considered when thinking about the process of remapping or restructuring, as well as any plans to create new critical infrastructure or facilities.

Institutionalize supply chain reviews. The U.S. government should institutionalize the use and frequency of supply chain reviews for critical sectors as part of a comprehensive framework to monitor and continuously improve supply chain resilience efforts. In addition to the 100-day supply chain reviews under the Biden administration's Executive Order 14017, periodic reviews would strengthen the capacity of relevant agencies to mitigate emerging supply chain risks and disruptions, as well as anticipate the impact of emerging technologies on supply chains.

Engage with industry leaders and private sector partners on the development and implementation of supply chain restructuring. Policymakers and government officials must continue to engage private sector partners and leverage existing models of public-private partnerships when considering the restructuring or remapping of critical supply chains. The U.S. government also should consult with industry leaders about the potential for onshoring critical manufacturing. Government funding also should be provided for pilot programs for supply chain diversification. Ultimately, private industry can help policymakers ensure a balance between national defense and economic security, while avoiding uncompetitive protectionism.

Leverage existing federal legislation and regulations to incentivize and drive transformation beneficial to the U.S. economy and defense. U.S. executive agencies have the authority to enforce, as well as regulate through supervision authorities in critical infrastructure, critical sectors related to U.S. defense or economic security. The U.S. government's available tools to drive and incentivize change include the Uyghur Forced Labor Prevention Act, sections 889 and 847 of the NDAA, sanctions imposed by the Department of the Treasury, the Foreign Investment Risk Review Modernization Act, and existing end-use control regulations.

Congress, in consultation with relevant government agencies, should:

Expand the use of existing industrial survey authorities. The Department of Commerce's Bureau of Industry and Security (BIS) has the authority under section 705 of the Defense Production Act to conduct "industry studies assessing the U.S. industrial base to support the national defense."[110] This authority should be amended to explicitly include supply chain–related information. Companies currently are providing such vital information on a voluntary basis. As a result, the quality and completeness of data are highly variable and temporal, impairing policymakers' ability to conduct sound planning and policy formulation.[111]

Promote efforts to improve software supply chain security. Existing governmental efforts to strengthen the resilience of supply chains should acknowledge and address software supply chain security. This effort could include a review of software supply chains, such as identifying potential vulnerabilities that come with critical software, as well as legislative proposals to map, monitor, and engage with partners and allies on issues relating to software security.

Evaluate vulnerabilities in U.S. stockpiles of critical materials and supplies for national defense. The U.S. government must prepare its strategic stockpiles for widespread disruption to global supply chains by increasing funding and resources for emergency preparedness and response. The Strategic National Stockpile, which can provide states with supplies and medicines in an emergency, and the U.S. National Defense Stockpile, which stores critical raw minerals and materials, both provide essential materials and supplies for U.S. national security. Government officials also should explore how the U.S. emergency reserves might support supply chain resiliency efforts. Finally, the U.S. government should increase funding and resources to allow for the adoption of data-driven prediction models and innovative approaches to emergency preparedness and response.

Encourage relevant government agencies to adopt emerging technologies, such as blockchain, to build transparency and accountability. Distributed ledger systems ensure transparency for all parties along a given supply chain by providing verifiable and certified information at every level of production. Blockchain technology in supply chains allows a limited number of known parties to access information throughout the entire stream, thereby increasing efficiency, trust, and visibility to all players in a supply chain.[112] Other emerging technologies, such as AI and big data analytics, can be used to strengthen transparency, optimize supply chains, and lower costs.

Identify, develop, and apply security principles for technologies in supply chains. As private industry continues to adopt emerging technologies such as 5G and Internet of Things infrastructure, cybersecurity concerns remain a persistent threat.[113] Congress in consultation with the Federal Communications Commission should review relevant principles for ensuring safe and secure usage of these technologies throughout critical supply chains.

Review and amend outdated provisions in the Uniform Commercial Code and others to optimize supply chain coordination. The governing legal standards for supply chains in the United States are based on the privity of contract doctrine, which prevents external parties and individuals from enforcing the obligations of a contract they are not a part of. This means parties affected by failures upstream are unable to take effective legal actions to remedy them. As supply chains become increasingly complex, it is necessary for legal foundations to evolve to support multiparty contractual agreements and enable main contractors to resolve issues within their supply chain.

Transform Supply Chains

For the U.S. government to craft and execute policies surrounding supply chain resilience, monitoring, and restructuring, it will need to implement a number of institutional changes across the government. The United States also will need to collaborate with allies and partners, both through existing partnerships and through new ones, to secure supply chains most critical to economic security and defense. To that end, Congress should:

Expand the mission of the Bureau of Industry and Security. BIS should assume authority to regulate and protect U.S. technology supply chains. It should be reorganized to model the Department of the Treasury's Office of Terrorism and Financial Intelligence.[114] Like the Department of the Treasury, the Commerce Department straddles the economic and national security arenas and is often tasked with handling nontraditional threats, including those posed to the U.S. technology supply chain. Despite the growing threat that supply chain vulnerabilities pose to the United States and the Commerce Department's expanding authority to address those concerns, there has not been a corresponding growth or interest in properly equipping the department to meet this challenge. A reorganization would centralize and consolidate the Department of Commerce's intelligence, policy, regulatory, and enforcement authorities related to the security of the technology supply chain.

Create an assistant secretary of commerce for supply chain and technology security. This position would centralize the department's policy and regulatory programs involving supply chain integrity, availability, and resilience, such as Defense Production Act programs, and planning and administration of BIS industry surveys. This action would be part of a broader move to expand the mission of the Bureau of Industry and Security.[115]

Congress, in conjunction with the State Department and the White House should:

Establish a network of like-minded countries to collaborate on technology policy.[116] Technology policy coordination among like-minded countries is often sporadic and disjointed. The United States should create a multilateral technology alliance with a core group of like-minded countries to collaborate on supply chain diversification.[117] This formal grouping of allied countries could focus efforts on securing and diversifying supply chains and bolstering information sharing to make critical supply chains more transparent. Additionally, this arrangement could discover new avenues for "friend-shoring"—allowing for globalized supply chains with trusted, geographically diverse suppliers.

Bolster U.S. capacity to conduct tech diplomacy. The United States needs a robust tech diplomacy capability to address the international dimensions of supply chains and technology competition more broadly. Unlike allies such as Australia, Denmark, and the Netherlands, the United States lacks a dedicated tech ambassador. Establishing a counterpart is essential to U.S. credibility on the world stage. To support the work of this new role, a new cadre of tech diplomats must be trained and assigned to a new entity, along the lines of the proposed Bureau of Cyberspace and Digital Policy or the International Technology Partnership Office.[118]

As a key player in any supply chain strategy, the Department of Commerce should:

Establish an information fusion center, headquartered in the International Trade Administration's Office of Industry and Analysis. Anticipating and mitigating supply chain risk will require a permanent and dedicated effort to monitor and analyze developments in industry and actions by foreign governments that impact supply chain dynamics. This function would be part of a broader mission of understanding foreign and domestic industrial and technological trends.

The NSF, in collaboration with relevant agencies, should:

Invest in next-generation tools, platforms, and technologies for supply chain security. For example, AI tools hold great promise to improve supply chain management such as by analyzing vast data sets, enhancing understanding of relationships, and supporting decision-making. Over the long term, breakthroughs in synthetic biology could result in an overhaul of manufacturing to create new onshore capacity, while the development of man-made materials with the properties of critical minerals could reduce or eliminate the need for mining and processing abroad. Interagency working groups, led by the NSF, DARPA, and other government departments and agencies, can provide insight in areas for research and development to reduce supply chain vulnerabilities. Alongside these investments for emerging tools and technologies, government agencies such as the Department of Commerce should work to integrate all of their open-source intelligence to ensure it is accessible, timely, and used effectively.

Conclusion

The breadth of the supply chain challenge is vast, and it will get only more complicated as time goes on. The United States must do what it can now, in conjunction with collaborative efforts with its allies and partners, to ensure its supply chains are resilient enough to withstand upheaval, geopolitical conflict, and natural disaster. How America secures its supply chains, and its effectiveness in doing so, will play a dominant role in U.S. economic and technological competitiveness with China.

As a key source of American economic advantage, defense, and sustained technological leadership, creating resilient and durable supply chains will remain a pressing national security issue for policymakers and private industry alike. Reevaluating and restructuring U.S. supply chains will require a clear and coherent long-term strategy—one that appreciates the balance between self-reliance and international partnerships, flexibility and efficiency, and diversity and security. A sound strategy is just the first step, however. Implementation is key. To keep pace with the increasingly complex global supply chain network, the United States must act now to identify and secure the supply chains it deems most critical to its security and prosperity.

1. Bureau of Industry and Security, U.S. Department of Commerce, U.S. *Industrial Base Surveys Pursuant to the Defense Production Act of 1950* (Washington: 2015), 41426, https://www.federalregister.gov/documents/2015/07/15/2015-17388/us-industrial-base-surveys-pursuant-to-the-defense-production-act-of-1950; Andrew J. Grotto, "U.S. Policy Toolkit for Kaspersky Labs," Lawfare, March 15, 2018, https://www.lawfareblog.com/us-policy-toolkit-kaspersky-labs.

2. Matt O'Brien, "As robots take over warehousing, workers pushed to adapt," Associated Press, December 30, 2019, https://apnews.com/article/connecticut-us-news-ap-top-news-az-state-wire-ct-state-wire-056b44f5bfff11208847aa9768f10757; Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, and Ali Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, 2021, https://link.springer.com/content/pdf/10.1007/s10207-021-00545-8.pdf.

3. John Costello, Martijn Rasser, and Megan Lamberth, "From Plan to Action: Operationalizing a U.S. National Technology Strategy," CNAS, July 29, 2021, https://www.cnas.org/publications/reports/from-plan-to-action.

4. Martijn Rasser and Megan Lamberth, "Taking the Helm: A National Technology Strategy to Meet the China Challenge," CNAS, January 13, 2021, https://www.cnas.org/publications/reports/taking-the-helm-a-national-technology-strategy-to-meet-the-china-challenge.

5. Martijn Rasser, Rebecca Arcesati, Shin Oya, Ainikki Riikonen, and Monika Bochert, "Common Code: An Alliance Framework for Democratic Technology Policy," CNAS, October 21, 2020, https://www.cnas.org/publications/reports/common-code.

6. Martijn Rasser and Megan Lamberth, "A plan to secure America's supply chains," *The Hill*, July 28, 2021, https://thehill.com/opinion/national-security/565209-a-plan-to-secure-americas-supply-chains.

7. House Armed Services Committee, *Report of the Defense Critical Supply Chain Task Force*, July 22, 2021, https://armedservices.house.gov/_cache/files/e/5/e5b9a98f-9923-47f6-a5b5-ccf77ebbb441/7E26814EA08F7F701B16D4C5FA37F043.defense-critical-supply-chain-task-force-report.pdf; The White House, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth*, June 2021, https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

8. For a detailed overview, see, for example: National Institute of Standards and Technology, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, 800-161, April 2015, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf.

9. "What's the Difference Between Sourcing and Procurement?" Procurement Cloud, December 1, 2021, https://kissflow.com/procurement/sourcing-vs-procurement/.

10. "The Significance of Tier 2 and Tier 3 Suppliers for Original Equipment Manufacturers (OEMs)," Universaldevlieg.com, https://www.universaldevlieg.com/blog/item/18-the-significance-of-tier-2-and-tier-3-suppliers-for-original-equipment-manufacturers-oems; Sophie Luo, "What is a Tier 1 Company or Supplier," *Insight*, December 18, 2021, https://insightsolutionsglobal.com/what-is-a-tier-1-company-or-supplier/; and Philipp Liegl, "What is a Tier Supplier?" Ecosio.com, July 13, 2021, https://ecosio.com/en/blog/what-is-a-tier-supplier/.

11. "Just in Time (JIT)," Chartered Institute of Procurement & Supply, https://www.cips.org/knowledge/procurement-topics-and-skills/operations-management/just-in-time/.

12. Jagdish Bhagwati, "Free Trade: Old and New Challenges," *The Economic Journal*, 104 no. 423 (March 1994), https://www.jstor.org/stable/pdf/2234745.pdf?casa_token=b6Qh133VuLUAAAAA:wMIz-bAI446M-9npBpvspFQ3bPVzkTF5nkdSgv3LZC8uGmoU-QRJSUD3DAVKSmT0sOSaPdamCF5IZi7Af_hBNEeNoF9b-CIbRqc8K-uQUlpGGUZdQ7LZFs-vA.

13. Dale C. Copeland, "Economic Interdependence and War: A Theory of Trade Expectations," *International Security*, 20 no. 4 (Spring 1996), https://www.jstor.org/stable/2539041?seq=2#metadata_info_tab_contents.

14. Thomas L. Friedman, *The World is Flat: A Brief History of the Twenty-first Century* (New York: Farrar, Straus and Giroux, 2005), https://www.amazon.com/World-Flat-History-Twenty-first-Century/dp/0374292884.

15. President Bill Clinton, "Full Text of Clinton's Speech on China Trade Bill," March 9, 2000, https://www.iatp.org/sites/default/files/Full_Text_of_Clintons_Speech_on_China_Trade_Bi.htm.

16. Kate O'Keeffe, Liza Lin, and Eva Xiao, "China's Export Restrictions Strand Medical Goods U.S. Needs to Fight Coronavirus, State Department Says," *The Wall Street Journal*, April 16, 2020, https://www.wsj.com/articles/chinas-export-restrictions-strand-medical-goods-u-s-needs-to-fight-coronavirus-state-department-says-11587031203.

17. Andrew Buncombe, "US and China in war of words as Beijing threatens to halt supply of medicine amid coronavirus crisis," *Independent*, March 13, 2020, https://www.independent.co.uk/news/world/americas/us-politics/coronavirus-china-us-drugs-trump-rubio-china-virus-xinhua-hell-epidemic-a9400811.html.

18. Sun Yu and Demetri Sevastopulo, "China targets rare earth export curbs to hobble US defence industry," *Financial Times*, February 16, 2021, https://www.ft.com/content/d3ed83f4-19bc-4d16-b510-415749c032c1.

19. Susan Helper and Evan Soltas, "Why the Pandemic Has Disrupted Supply Chains," the White House, June 17, 2021, https://www.whitehouse.gov/cea/blog/2021/06/17/why-the-pandemic-has-disrupted-supply-chains/.

20. Jenn Fulmer, "The End of the Just in Time Supply Chain Method," Baseline, May 3, 2021, https://www.baselinemag.com/it-management/end-of-just-in-time-supply-chain-method.html; Peter S. Goodman and Niraj Chokshi, "How the World Ran Out of Everything," *The New York Times*, June 1, 2021, https://www.nytimes.com/2021/06/01/business/coronavirus-global-shortages.html.

21. Hong Chen, Owen Q. Wu, and Murray Z. Frank, "What Actually Happened to the Inventories of American Companies Between 1981 and 2000?" *Management Science*, July 2005, https://www.researchgate.net/profile/Murray-Frank/publication/220535200_What_Actually_Happened_to_the_Inventories_of_American_Companies_Between_1981_and_2000/links/00b7d526148a133fb2000000/What-Actually-Happened-to-the-Inventories-of-American-Companies-Between-1981-and-2000.pdf; Goodman and Chokshi, "How the World Ran Out of Everything."

22. Goodman and Chokshi, "How the World Ran Out of Everything."

23. Sam Shead, "The global chip shortage is starting to have major real-world consequences," CNBC, May 7, 2021, https://www.cnbc.com/2021/05/07/chip-shortage-is-starting-to-have-major-real-world-consequences.html.

24. Knut Alicke, Richa Gupta, and Vera Trautwein, "Resetting supply chains for the next normal," McKinsey & Company, July 21, 2020, https://www.mckinsey.com/business-functions/operations/our-insights/resetting-supply-chains-for-the-next-normal.

25. Jonathan M. Gitlin, "A silicon chip shortage is causing automakers to idle their factories," *Ars Technica*, February 4, 2021, https://arstechnica.com/cars/2021/02/a-silicon-chip-shortage-is-causing-automakers-to-idle-their-factories/.

26. Helper and Soltas, "Why the Pandemic Has Disrupted Supply Chains."

27. Helper and Soltas, "Why the Pandemic Has Disrupted Supply Chains."

28. "Shortages Related to Semiconductors to Cost the Auto Industry $210 Billion in Revenues This Year, Says New Alixpartners Forecast," AlixPartners press release, September 23, 2021, https://www.alixpartners.com/media-center/press-releases/press-release-shortages-related-to-semiconductors-to-cost-the-auto-industry-210-billion-in-revenues-this-year-says-new-alixpartners-forecast/; William Boston, "Volkswagen Sees Global Chip Shortage Worsening in Second Half," *The Wall Street Journal*, July 9, 2021, https://www.wsj.com/articles/volkswagen-sees-global-chip-shortage-worsening-in-second-half-11625861486.

29. Neal E. Boudette, "Ford profit drops 50 percent because of a global chip shortage," *The New York Times*, July 28, 2021, https://www.nytimes.com/2021/07/28/business/ford-q2-earnings.html.

30. Neal E. Boudette, "Toyota, hurt by the chip shortage, will reduce output 40 percent in September," *The New York Times*, August 19, 2021, https://www.nytimes.com/2021/08/19/business/toyota-production-slowdown-chip-shortage.html.

31. Dan Bilefsky and Ana Swanson, "Automakers Are Hobbled by Blockades at U.S.-Canada Border," *The New York Times*, February 10, 2022, https://www.nytimes.com/live/2022/02/10/world/protests-in-canada.

32. Brooke Masters and Andrew Edgecliffe-Johnson, "Supply chains: companies shift from 'just in time' to 'just in case,'" *Financial Times*, December 20, 2021, https://www.ft.com/content/8a7cdc0d-99aa-4ef6-ba9a-fd1a1180dc82.

33. Semiconductor Industry Association, "Written Comments from the Semiconductor Industry Association," April 5, 2021, https://www.semiconductors.org/wp-content/uploads/2021/04/4.5.21-SIA-supply-chain-submission.pdf.

34. Semiconductor Industry Association, "Written Comments from the Semiconductor Industry Association."

35. Stephen Nellis, "Global chip supply chain increasingly vulnerable to massive disruption, study finds," Reuters, April 1, 2021, https://www.reuters.com/article/us-usa-semiconductors/global-chip-supply-chain-increasingly-vulnerable-to-massive-disruption-study-finds-idUSKBN2BO4TV.

36. Bill Canis, "The Motor Vehicle Supply Chain: Effects of the Japanese Earthquake and Tsunami," R41831, Congressional Research Service, May 23, 2011, https://sgp.fas.org/crs/misc/R41831.pdf.

37. Peter S. Goodman, "Hurricane Ida could make the supply chain disaster even worse," *The New York Times*, August 31, 2021, https://www.nytimes.com/2021/08/31/business/hurricane-ida-supply-chain-shortages.html.

38. Diana Olick, "Climate change will disrupt supply chains much more than Covid—here's how businesses can prepare," CNBC, August 19, 2021, https://www.cnbc.com/2021/08/19/climate-change-supply-chain-disruptions-how-to-prepare.html.

39. Olick, "Climate change will disrupt supply chains much more than Covid."

40. Christopher M. Matthews, Austen Hufford, and Collin Eaton, "Texas Freeze Triggers Global Plastics Shortage," *The Wall Street Journal*, March 17, 2021, https://www.wsj.com/articles/one-week-texas-freeze-seen-triggering-monthslong-plastics-shortage-11615973401.

41. Motoko Rich, Stanley Reed and Jack Ewing, "Clearing the Suez Canal Took Days. Figuring Out the Costs May Take Years," *The New York Times*, March 31, 2021, https://www.nytimes.com/2021/03/31/business/suez-canal-ship-costs.html.

42. Ido Vock, "The Suez Canal blockage is a reminder that geography does matter in trade," *The New Statesman*, March 29, 2021, https://www.newstatesman.com/world/2021/03/suez-canal-blockage-reminder-geography-does-matter-trade.

43. Helper and Soltas, "Why the Pandemic Has Disrupted Supply Chains."

44. Keith Bradsher and Liz Alderman, "The World Needs Masks. China Makes Them, but Has Been Hoarding Them," *The New York Times*, March 13, 2020, https://www.nytimes.com/2020/03/13/business/masks-china-coronavirus.html.

45. Martijn Rasser, "Pandemic Problem: America's Supply Chains are Dangerously Brittle," *The National Interest*, March 17, 2020, https://nationalinterest.org/feature/pandemic-problem-americas-supply-chains-are-dangerously-brittle-134022.

46. Yanzhong Huang, "The Coronavirus Outbreak Could Disrupt the U.S. Drug Supply," Council on Foreign Relations, March 5, 2020, https://www.cfr.org/in-brief/coronavirus-disrupt-us-drug-supply-shortages-fda.

47. "Fact Sheet: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities," White House press release, June 8, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/.

48. The White House, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth*.

49. Sara Hsu, "Which Asian Nations Can Benefit From the 'China Plus One' Strategy?" *The Diplomat*, June 11, 2021, https://thediplomat.com/2021/06/which-asian-nations-can-benefit-from-the-china-plus-one-strategy/; Willy C. Shih, "Global Supply Chains in a Post-Pandemic World," *Harvard Business Review*, September-October 2020, https://hbr.org/2020/09/global-supply-chains-in-a-post-pandemic-world.

50. Tom Linton and Bindiya Vakil, "Coronavirus is Proving We Need More Resilient Supply Chains," *Harvard Business Review*, March 5, 2020, https://hbr.org/2020/03/coronavirus-is-proving-that-we-need-more-resilient-supply-chains?registration=success.

51. Alexis Bateman and Leonardo Bonanni, "What Supply Chain transparency Really Means," *Harvard Business Review*, August 20, 2019, https://hbr.org/2019/08/what-supply-chain-transparency-really-means.

52. Patrick Burnson, "Oracle Survey Indicates Supply Chain Glitches Are Alarming to Consumers," *Supply Chain Management Review*, October 5, 2021, https://www.scmr.com/article/oracle_survey_indicates_supply_chain_glitches_are_alarming_to_consumers.

53. Burnson, "Oracle Survey Indicates Supply Chain Glitches Are Alarming to Comsumers."

54. Alexis Bateman and Leonardo Bonanni, "What Supply Chain Transparency Really Means," *Harvard Business Review*, January 20, 2021, https://hbr.org/2019/08/what-supply-chain-transparency-really-means.

55. Bateman and Bonanni, "What Supply Chain Transparency Really Means"; Tim Kraft, León Valdés, and Yanchong Zheng, "Supply Chain Visibility and Social Responsibility: Investigating Consumers' Behaviors and Motives," *Manufacturing & Service Operations Management 20*, no. 4 (October 9, 2017), pp. 617–636: https://www.semanticscholar.org/paper/Supply-Chain-Visibility-and-Social-Responsibility%3A-Kraft-Vald%C3%A9s/29d0dd5daedde45e414a07ba170d6243ccbf89d4.

56. Ana Swanson, "U.S. Bans All Cotton and Tomatoes from Xinjiang Region of China," *The New York Times*, January 13, 2021, https://www.nytimes.com/2021/01/13/business/economy/xinjiang-cotton-tomato-ban.html; Annachiara Biondi, "Fashion's Cotton Supply Caught in Crossfire of US-China Trade War," *Vogue Business*, September 16, 2020, https://www.voguebusiness.com/sustainability/us-ban-cotton-xinjiang.

57. Eva Dou, Jeanne Whalen, and Alicia Chen, "U.S. Ban on China's Xinjiang Cotton Fractures Fashion Industry Supply Chains," *The Washington Post*, February 22, 2021, https://www.washingtonpost.com/world/asia_pacific/china-cotton-sanctions-xinjiang-uighurs/2021/02/21/a8a4b128-70ee-11eb-93be-c10813e358a2_story.html.

58. Swanson, "U.S. Bans All Cotton and Tomatoes from Xinijuang Region of China"; Dou, Whalen, and Chen, "U.S. Ban on China's Xinjiang Cotton Fractures Fashion Industry Supply Chains."

59. "What Is the Food Safety Modernization Act (FSMA)?" National Sustainable Agriculture Coalition, May 23, 2018, https://sustainableagriculture.net/fsma/overview-and-background/.

60. "Food Safety Modernization Act (FSMA)," Center for Food Safety and Applied Nutrition, U.S. Food and Drug Administration, https://www.fda.gov/food/guidance-regulation-food-and-dietary-supplements/food-safety-modernization-act-fsma.

61. John T Shapiro, "Traceability Is Not a Substitute for Transparency in the Recipe for Food Company Success," *Food Safety Maganize*, February 22, 2016, https://www.food-safety.com/articles/3999-traceability-is-not-a-substitute-for-transparency-in-the-recipe-for-food-company-success.

62. Andy Pulling, "Food Safety Modernization Act – Where Are We Now?" Aptean, April 2, 2020, https://www.aptean.com/en-US/insights/blog/food-safety-modernization-act-where-are-we-now; Frank Yiannas, "A Decade Later, FDA Still Working on Congressional Mandate Known as FSMA," *Food Safety News*, April 8, 2021, https://www.foodsafetynews.com/2021/01/199987/; "FSMA Overview," NC State Extension News, https://foodsafetyprocessors.ces.ncsu.edu/fsma-overview/.

63. Susan Lund et al., "Risk, resilience, and rebalancing in global supply chains," McKinsey Global Institute, August 6, 2020, https://www.mckinsey.com/business-functions/operations/our-insights/risk-resilience-and-rebalancing-in-global-value-chains; Bateman and Bonanni, "What Supply chain Transparency Really Means."

64. Bateman and Bonanni, "What Supply chain Transparency Really Means."

65. Bateman and Bonanni, "What Supply chain Transparency Really Means."

66. Helper and Soltas, "Why the Pandemic Has Disrupted Supply Chains."

67. Martijn Rasser, "Pandemic Problem: America's Supply Chains Are Dangerously Brittle," *The National Interest*, March 18, 2020, https://nationalinterest.org/feature/pandemic-problem-americas-supply-chains-are-dangerously-brittle-134022.

68. Neil Hume, "China's Magnesium Shortage Threatens Global Car Industry," *Financial Times*, October 19, 2021, https://www.ft.com/content/1611e936-08a5-4654-987e-664f50133a4b.

69. The White House, *Executive Order on America's Supply Chains*, February 24, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

70. Peter Coy, "'Onshoring' Is So Last Year. The New Lingo Is 'Friend-Shoring,'" Bloomberg, June 24, 2021, https://www.bloomberg.com/news/articles/2021-06-24/-onshoring-is-so-last-year-the-new-lingo-is-friend-shoring.

71. This exponential growth of semiconductors is due to Moore's Law, which stipulates the capabilities of semiconductors traditionally double every two years while costs continually decrease. Fifty years after it was coined, Moore's Law remains remarkably robust and in some ways a self-fulfilling prophecy. As transistor density continues to increase, though, semiconductors are approaching a terminal density and will require further innovation.

72. Dave Nyczepir, "Lagging Hardware Could Hinder US Quantum Ambitions," *FedScoop*, October 5, 2021, https://www.fedscoop.com/hardware-u-s-quantum-ambitions/.

73. Anna Slomovic, "An analysis of military and commercial microelectronics: Has DoD's R&D funding had the desired effect?" PhD thesis, 1991, https://www.rand.org/content/dam/rand/pubs/notes/2009/N3318.pdf.

74. Larry D. Browning, Janice M. Beyer, and Judy C. Shetler, "Building Cooperation in a Competitive Industry: SEMATECH and the Semiconductor Industry," *Academy of Management Journal*, 38 no. 1 (February 1995), https://www.jstor.org/stable/pdf/256730.pdf?refreqid=excelsior%3A3977921bca5d80977ce64d2c88bcf267&ab_segments=&origin=, 113–151.

75. Robert D. Hof, "Lessons from Sematech," *MIT Technology Review*, February 1, 2020, https://www.technologyreview.com/2011/07/25/192832/lessons-from-sematech/.

76. Hof, "Lessons from Sematech."

77. "Research and Development Expenditure (% of GDP)—China, United States," the World Bank, https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=CN-US.

78. Amar Diwakar, "'Chip Wars': US, China and the Battle for Semiconductor Supremacy," *TRT World*, March 16, 2021, https://www.trtworld.com/magazine/chip-wars-us-china-and-the-battle-for-semiconductor-supremacy-45052.

79. Yasmin Tadjdeh, "Semiconductor Shortage Shines Light On Weak Supply Chain," *National Defense*, May 21, 2021, https://www.nationaldefensemagazine.org/articles/2021/5/21/semiconductor-shortage-shines-light-on-weak-supply-chain.

80. "Chips for America Act & Fabs Act," Semiconductor Industry Association, https://www.semiconductors.org/chips/.

81. Saheli Roy Choudhury, "Tough Road Ahead for U.S. Firms Trying to Cut Reliance on Taiwan Chipmakers," CNBC, April 13, 2021, https://www.cnbc.com/2021/04/13/semiconductor-shortage-us-tech-companies-and-their-reliance-on-taiwan.html.

82. Michael Reid and Falan Yinug, "Chipping In: The Positive Impact of the Semiconductor Industry on the American Workforce and How Federal Industry Incentives Will Increase Domestic Jobs," Semicondcutor Industry Assoication, May 2021, https://www.semiconductors.org/wp-content/uploads/2021/05/SIA-Impact_May2021-FINAL-May-19-2021_2.pdf, 5.

83. Matthew Thibault, "Intel to Build 2 Ohio Semiconductor Factories Worth $20B," *Construction Dive*, January 26, 2022, https://www.constructiondive.com/news/intel-to-build-2-ohio-semiconductor-factories-worth-20b/617718/.

84. Eric Chang, "Taiwan semiconductor production on pace for record growth in 2021," *Taiwan News*, November 29, 2021, https://www.taiwannews.com.tw/en/news/4359446.

85. National Research Council, *Securing the Future: Regional and National Programs to Support the Semiconductor Industry*, (Washington: National Academies Press, 2003).

86. National Research Council, *Securing the Future*.

87. National Research Council, *Securing the Future*.

88. "Taiwan Semiconductor Manufacturing Company Ltd. History," Fundinguniverse.com, http://www.fundinguniverse.com/company-histories/taiwan-semiconductor-manufacturing-company-ltd-history/.

89. Cheng Ting-Fang and Lauly Li, "Taiwan to invest $300m in grad schools to stem chip rain drain," *Nikkei Asia*, January 16, 2021, https://asia.nikkei.com/Business/Tech/Semiconductors/Taiwan-to-invest-300m-in-grad-schools-to-stem-chip-brain-drain.

90. Nicolás Rivero, "The global semiconductor shortage can be explained by the bullwhip effect," Quartz, May 5, 2021, https://qz.com/2004569/the-global-chip-shortage-can-be-explained-by-the-bullwhip-effect/.

91. Ian King, "Chip Delivery Times Are on the Rise Again, Shortages to Continue," Bloomberg, January 4, 2022, https://www.bloomberg.com/news/articles/2022-01-04/chip-delivery-times-are-on-the-rise-again-shortages-to-continue.

92. Representative Michael T. McCaul, "H.R.7178 - CHIPS for America Act," https://www.congress.gov/bill/116th-congress/house-bill/7178.

93. Larry D. Browning, Janice M. Beyer, and Judy C. Shetler, "Building Cooperation in a Competitive Industry: SEMATECH and the Semiconductor Industry," *The Academy of Management Journal*, 28 no. 1 (February 1995), https://www.jstor.org/stable/pdf/256730.pdf?refreqid=excelsior%3A3977921bca5d80977ce64d2c88bcf267&ab_segments=&origin=.

94. Trey Herr, Will Loomis, Emma Schroeder, Stewart Scott, Simon Handler, and Tianjiu Zuo, "Broken trust: Lessons from Subnurst," Atlantic Council, March 29, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/.

95. U.S. Government Accountability Office, Software Development: *DOD Faces Risks and Challenges in Implementing Modern Approaches and Addressing Cybersecurity Practices*, GAO-21-351, June 23, 2021, https://www.gao.gov/products/gao-21-351.

96. U.S. Government Accountability Office, *Software Development*.

97. Jack Corrigan, "The Pentagon's Drones May Soon Run on Open Source Software," Nextgov, May 2, 2019, https://www.nextgov.com/emerging-tech/2019/05/pentagons-drones-may-soon-run-open-source-software/156684/; National Security Agency and Cybersecurity and Infrastructure Security Agency, "Selecting and Hardening Remote Access VPN Solutions," September 2021, https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF.

98. "Open Source Libraries & Security Vulnerabilities," QualityClouds, January 14, 2022, https://www.qualityclouds.com/open-source-libraries-and-security-vulnerabilities/.

99. Nicolás Rivero, "What is a supply chain cyber attack?" Quartz, July 6, 2021, https://qz.com/2030053/what-is-a-supply-chain-cyber-attack/.

100. John F. Miller, "Supply Chain Attack Framework and Attack Patterns," MITRE, December 2013, https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf.

101. Lucian Constantin, "SolarWinds attack explained: And why it was so hard to detect," CSO, December 15, 2020, https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html.

102. Herr, Loomis, Schroeder, Scott, Handler, and Zuo, "Broken trust: Lessons from Subnurst."

103. "Understanding the increase in Supply Chain Security Attacks," European Union Agency for Cybersecurity press release, July 29, 2021, https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks.

104. "Understanding the increase in Supply Chain Security Attacks."

105. "2021 CrowdStrike Global Security Attitude Survey," CrowdStrike, 2021, https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021CSGlobalSecurityAttitudeSurvey.pdf.

106. The White House, *Executive Order on Ensuring the Future is Made in All of America by All of America's Workers*, (January 25, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/25/executive-order-on-ensuring-the-future-is-made-in-all-of-america-by-all-of-americas-workers/; Makenzie Holland and Patrick Thibodeau, "Biden wants review of IT exemptions in Buy American law," TechTarget, February 4, 2021, https://searchcio.techtarget.com/feature/Biden-wants-review-of-IT-exemption-in-Buy-American-law.

107. House Armed Services Committee, *Report of the Defense Critical Supply Chain Task Force*.

108. *Artificial Intelligence and Cybersecurity: Opportunities and Challenges*, National Science and Technology Council, March 2020, https://www.nitrd.gov/pubs/AI-CS-Tech-Summary-2020.pdf.

109. "New, free tool adds layer of security for the software supply chain," NYU Tandon School of Engineering press release, December 15, 2020, https://engineering.nyu.edu/sites/default/files/2020-12/In-Toto-release.pdf; "What is in-toto?," in-toto.io, https://in-toto.io/in-toto/.

110. Bureau of Industry and Security, U.S. Department of Commerce, *U.S. Industrial Base Surveys Pursuant to the Defense Production Act of 1950* (Washington: 2015), 41426, https://www.federalregister.gov/documents/2015/07/15/2015-17388/us-industrial-base-surveys-pursuant-to-the-defense-production-act-of-1950; Andrew J. Grotto, "U.S. Policy Toolkit for Kaspersky Labs," Lawfare, March 15, 2018, https://www.lawfareblog.com/us-policy-toolkit-kaspersky-labs.

111. The White House, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth*.

112. Vishal Gaur and Abhinav Gaiha, "Building a Transparent Supply Chain," *Harvard Business Review*, May-June 2020, https://hbr.org/2020/05/building-a-transparent-supply-chain.

113. O'Brien, "As robots take over warehousing, workers pushed to adapt"; Yaacoub, Noura, Salman, and Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations."

114. Costello, Rasser, and Lamberth, "From Plan to Action.

115. Costello, Rasser, and Lamberth, "From Plan to Action.."

116. Rasser and Lamberth, "Taking the Helm."

117. Rasser, Arcesati, Oya, Riikonen, and Bochert, "Common Code."

118. Matthew Willoughby, "A Commitment to Modernizing American Diplomacy," state.gov, October 28, 2021, https://www.state.gov/dipnote-u-s-department-of-state-official-blog/a-commitment-to-modernizing-american-diplomacy/; Senator Mark R. Warner, "S.604 - Democracy Technology Partnership Act," https://www.congress.gov/bill/117th-congress/senate-bill/604?s=1&r=8.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, DC, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan.


Center for a
New American
Security