Foreign Policy at BROOKINGS

Building greater resilience and capacity in the US national security industrial base

Michael E. O'Hanlon, Marta E. Wosińska, Mark Muro, and Thomas Wright

Photo: Airman 1st Class Mikaela Smith/U.S. Air Force via DVIDS

Building greater resilience and capacity in the US national security industrial base

Michael E. O'Hanlon, Marta E. Wosińska, Mark Muro, and Thomas Wright

Contents

In the current policy landscape, virtually every stakeholder—from federal agencies to industry groups—calls for classifying a widening swath of economic activity as "national security." The impulse to broaden what counts as critical has gained momentum not only with each new global disruption, but also with each new report highlighting U.S. exposure to China in key sectors, making "national security" a catchall for fears that range from supply interruptions to cyber threats. While this instinct reflects real vulnerabilities, it leaves policymakers struggling to prioritize and risks making the label so expansive that it ceases to have sharp policy meaning.

This paper cuts through that noise. We agree with the notion of expanding the concept of national security to include production supply chains, the interruption of which by a hostile foreign actor could directly imperil large numbers of American lives or the functioning of society. Our approach, however, is not simply whether to broaden the concept of national security, but how to realistically *scope* it—especially when it comes to supply chains. (We leave debates about expanding the framework to cover topics like cyber or information influence for other venues.) Our premise is simple: Yes, we need to think about more than the defense industrial base when deciding which sectors of the economy are within a broader "national security industrial base," and accordingly are protected or strengthened. Yet without disciplined prioritization, government efforts risk becoming fragmented, inefficient, and ultimately unable to protect what matters most.

Multiple legislative efforts—from the Promoting Resilient Supply Chains Act in Congress to new mapping initiatives from the Department of Defense (DOD) and Commerce Department—attest to Washington's determination to reduce exposure to adversaries and harden fragile supply lines. But with so many agencies, industries, and sectors seeking "critical" designation, the path from mapping everything to protecting anything remains unclear.

This paper proposes a disciplined framework to help policymakers navigate these choices. We focus on supply chains—where physical disruption, not just digital attack, can quickly undermine military readiness, economic stability, or the population's health and safety. We further direct our focus to supply chains at potential risk due to actions by hostile foreign actors (as opposed to natural disasters, for example, though improving resilience against natural disasters is also important, of course). Our main focus is on the potential physical interruption of supply chains, rather than vulnerabilities to either natural disaster or cyberattack, though we do note several cases where cybersecurity considerations would argue for rethinking certain supply chains. We offer clear criteria and sectoral context to distinguish risks that truly rise to the level of national security from those with a less direct, mainly economic or commercial effect.

We argue that supply chains are a national security matter when these three conditions coincide:

1. Supply chain disruption caused by an adversary would rapidly threaten lives, national defense, or essential economic sectors.

2. Substitutes are unavailable or cannot be mobilized quickly.

3. Building surge capacity through allies or domestic investment is not realistic in relevant timeframes.

Importantly, we do not argue for self-sufficiency in all things, nor do we ignore other potential vulnerabilities such as those in cyber; rather, we focus on those physical and productive supply chain bottlenecks that—if left unaddressed—could be exploited in a conflict or crisis.

This paper is organized as follows. The next section discusses the traditional approach to supply chains and national security, namely, the supply chains supporting the DOD military industrial base. The country is making progress in strengthening these sectors, including through DOD initiatives as well as the CHIPS and Science

Act of 2022, but a good deal more remains to be done. We then discuss a framework for rightsizing an expansion of the national security framework to encompass civilian supply chains. Next, we apply the framework to the remaining 15 sectors already designated by the U.S. government as critical infrastructure and identify where vulnerabilities with national security implications may currently exist. We follow the sector analysis by identifying cross-cutting supply chain vulnerabilities that may affect multiple sectors. We conclude with a set of recommendations for next steps in advancing the proposed framework.

The military industrial base

The Department of Defense relies on a vast and diverse military or defense industrial base—the network of public and private organizations, facilities, and suppliers that research, develop, produce, and deliver the full range of products and services needed for U.S. military acquisition, readiness, and operations. The defense industrial base encompasses everything from sophisticated weapons platforms to basic essentials, sustaining the armed forces with tanks, aircraft, ammunition, uniforms, food, and advanced medical equipment and pharmaceuticals.

Despite the broad supply chain exposure, DOD was not always a great trailblazer on the subject of securing supply chains. In some ways, it was the exact opposite. At the famous "last supper" dinner in the early 1990s, after the Cold War had ended, DOD officials told the gathered crowd of industry executives that they should take it upon themselves to consolidate with an eye toward reducing redundancy and maximizing efficiency. This message was not all wrong, especially for that moment. However, it was implemented too narrowly for too many decades to come.[1] What resulted was many of the problems we have today: dependencies on certain unreliable foreign suppliers, potential bottlenecks and single points of failure, and a lack of surge capacity.

Fortunately, things are now moving in a better direction, thanks mostly to the last two U.S. administrations and the Congresses that worked with them.

A pathbreaking 2022 Pentagon document on the defense industrial base, ironically released the day that Russia initiated its major attack on Ukraine, identified four technology areas where the DOD determined that it had particular weaknesses. They included castings and forgings for metals and composites, batteries and energy storage, microelectronics, and the general category of "kinetic" capabilities to include explosives, rockets and rocket fuel, hypersonic weapons, and (seemingly somewhat out of place) directed energy weapons. This list, though uneven in scope and specificity, was nonetheless a useful starting point in determining where the Pentagon might choose to direct and redirect resources to create additional sources of supply.[2]

In parallel, that report also underscored the need for greater transparency and visibility into sub-tier suppliers, since the DOD had largely relied on prime contractors themselves to monitor their own production networks. Alas, even contractors often lose visibility into who produces what below the third tier of producers (that is, sub-contractors to sub-contractors); they also may fail to recognize situations in which several primes depend on the same small number of subcontractors in a given technology area.[3]

The 2023 National Defense Industrial Strategy (NDIS) provided a more detailed framework for how to understand vulnerabilities in the defense industrial base as well as the tools that might strengthen it. It emphasizes several possible approaches to strengthen supply chains and increase resilience as well as surge capacity: deliberately creating excess industrial capacity even at some cost, promoting flexible manufacturing that can pivot to defense needs as necessary, expanding public-private partnerships for production of some goods, providing assistance for small businesses trying to work with the Pentagon but getting overwhelmed by regulation and paperwork, deepening the defense workforce, and promoting greater allied capabilities.[4]

A third key recent Pentagon document, the 2024 NDIS Implementation Plan, underscored the importance of deepening and broadening supply networks for munitions, submarines, small robotics (including through the Replicator initiative), and basic commodities in the National Defense Stockpile. The implementation plan designated lead agencies within the DOD and the broader government for each type of key technology or capability. It also estimated the funds that were already being dedicated annually to each line of effort. Total figures added up into the tens of billions of dollars a year—large sums, suggesting double-counting of numerous programs or priorities that were already underway, as opposed to new and targeted interventions. In any event, it was more a tallying of inputs than a presentation of outputs and generally lacked metrics that could be used to assess progress toward strengthening the industrial base. (A classified annex may have more hard data, but we do not know.)[5]

Based on these documents and other sources of data, what first impressions can we offer about the basic state of the U.S. defense industrial base today?

Several categories of industrial capability, to include castings, forgings, batteries, and microelectronics, as well as rare earth metals and magnets, are either acquired abroad or from a very narrow contractor and subcontractor base. Some of these weaknesses have been identified and are being addressed, for example, through a combination of "patriotic" investors and DOD-backed venture capital in which the U.S. government becomes part owner of an operation and potentially guarantees a minimal price for its output.[6]

Often, however, the government still does not fully see or understand such vulnerabilities because it only has limited information on third-tier, fourth-tier, and fifth-tier contractors and suppliers. Most efforts to mitigate these vulnerabilities are in their infancy. The Department of Defense seems better at measuring inputs in the form of subsidies and the like than at assessing the pace of progress toward greater capacity and resiliency in the defense industrial base.

Although this point is somewhat tangential to the question of supply chain vulnerability to foreign interference, it is worth noting that in many cases, the United States depends on a single shipyard or main factory to produce a given type of major weapons platform. It is dubious that even full execution of the DOD defense industrial base strategy implementation plan would change the situation in all cases. A devastating attack on such a facility, or some natural catastrophe afflicting it, could put the country in a difficult position very quickly. Production facilities or operating bases for Virginia-class attack submarines, Ohio-class and Columbia-class nuclear-armed submarines, B-21 bombers, F-35 aircraft, aircraft carriers, and several other expensive and exquisite ships, planes, rockets, or aircraft make the United States quite vulnerable to certain types of possible hostile action (not to mention natural catastrophe in some cases, as well).

In conclusion, while the DOD is making headway, it is generally better now at understanding its problems than at solving them. Efforts to achieve redress remain in early stages in general. In addition, the danger of relying on largely invisible third-tier and fourth-tier subcontractors must be mitigated. Perhaps a new classification system that would protect data collected about such subcontractors should be created, with only a small number of people in the DOD authorized to access it to respect the proprietary interests of the various companies involved. Those DOD officials should also have resources at their beck and call to address vulnerabilities, inadequacies, or bottlenecks when they are discovered.

A word on key raw materials

Before moving on to a broader consideration of critical national infrastructure and of the national security industrial base writ large, a further word is in order on key raw materials. These are relevant to the defense industrial base as well as the broader national security industrial base. The concern is particularly acute in cases where China is the main U.S. source of raw or refined materials, such as rare earth minerals. Beijing's willingness to deprive Japan of such materials some 15 years ago over a dispute over the Senkaku/Diaoyu islands and its willingness to leverage rare earth magnets against President Donald Trump in 2025 should provide ample warning signs of the potential for future trouble. There is at present only one working mine in North America for rare earths—and these are then shipped to China for processing. There are no such mines in Europe; any development of assets in Greenland is happening only very slowly.[7]

Given the slow pace of progress in expanding capacity, the best response to this set of U.S. (and allied) vulnerabilities might include near-term stockpiling of rare earth minerals and certain other crucially important commodities while continuing with the longer-term development of alternative sources, in North America and elsewhere, and in developing alternative processing locations. Doing the latter will not always require the establishment of completely new extraction sites. In fact, on the subject of rare earths, a considerable quantity of material is already being mined—but then discarded—in domestic exploitation of resources like gold. Various kinds of subsidies or other incentives could be considered so that companies already digging up rare earth minerals would have reason to collect and process them.[8]

This is not a brand-new problem; it was taken seriously during the Cold War. Restoring the U.S. National Defense Stockpile for key raw materials toward its Cold War level of $15 billion (today, it is a factor of 10 less) could be a prudent step. That is admittedly just a ballpark number; dependencies are of a different degree and kind today, given the evolution of technology.[9] But it gives an illustrative figure—and a reminder that stockpiling, for minerals and metals (as well as some chemicals, transformers, and certain other aforementioned assets) represents a straightforward way to buy time in economic sectors where that is an adequate response to vulnerable supply chains.

Broadening, but disciplining, the National Security Industrial Base

We would submit that the concept of U.S. national security has been defined too narrowly in the past, as has the associated idea of the national security industrial base. That said, it is crucial in this era of a greater governmental role in the economy that we not label virtually every sector of the economy as crucial to American national security.[10] There is a danger that we could collectively overdo it. There are strong arguments in favor of promoting advanced industry in general, for economic growth, high-wage workforce development, and national economic and technological leadership writ large.[11] But we are, again, focused on a more specific problem, that of U.S. national security.

National security should not be seen as just a question of preventing an enemy from seizing American territory or causing grievous harm to American populations through direct physical

attack. We would propose this definition of U.S. national security: the country's ability to protect its territory, its people, and the normal functioning of its society from hostile adversarial action of any type.

By that definition, most dangers to the economy or to individual Americans, however serious, would not be viewed as matters of national security. The danger of defining the national security industrial base too loosely is that we can waste huge amounts of resources protecting everything, while failing to protect what is truly crucial. But many things beyond direct battlefield attack could constitute serious national security matters.

For example, the United States has come to depend upon China for inputs to prescription drugs taken by more than half of the adult U.S. population.[12] [13] Were a war to occur over Taiwan, might Beijing threaten to cut off shipments of such supplies if the United States were to enter the conflict on Taiwan's side? It might seem inhumane that a foreign rival would take this step, but as the saying goes, there are no rules (or few rules) in matters of love and of war. After all, the United States itself deliberately targeted Japanese populations in World War II in an attempt to end the conflict, when the alternative means of ending the war were bleak. If we Americans could do it then, what makes us so sure that an enemy would not turn the tables on us in the future?

Shipbuilding provides another example. Being able to produce warships is clearly of significance for national security. Being able to produce commercial ships, by contrast, is less crucial—many are built by friendly nations, and in the event of some disruption to supply, existing ships are numerous and can, in many cases, have their lifetimes extended. That said, for military purposes in a protracted war, the nation probably needs greater shipbuilding capacity of all types than it has today. Commercial shipbuilding capacity can be viewed in some sense as latent military production capacity for times of national security crisis. Without it, expanding the naval shipbuilding industrial base in times of war would likely be a multiyear process, arguably far too long to wait. It is in something of a gray zone of national security relevance, but closer to being a national security matter than not.

These distinctions are not meant to be mere semantics. Figuring out what is a potential national security threat is important for policy. If would-be adversaries understand our weaknesses, they can target them. Our job in peacetime is to anticipate such action and adopt appropriate preventive measures in the interest of deterrence, as well as resilience, should conflict take place.

If it were luxuries or conveniences at issue, a potential interruption to production would likely not qualify as a national security matter. For example, production of most consumer durables should not be associated with the national security industrial base. If supplies were interrupted, reasonable (if potentially painful or inconvenient) countermeasures would likely be available to the nation, including prolonging the lives of existing products, substituting for them, simply doing without them in some cases, and gradually building up domestic production capacity as a substitute for previous foreign supply.

But production capabilities affecting the basic functioning of society, its core infrastructure, and the basic safety and security of its citizens would be captured within the proper scope of national security matters. That could include electricity, communications, water, sewage, chemical, and transportation infrastructure, for example.

The recent discussion about metal production in the United States is relevant here as well. The idea of keeping U.S. Steel in American hands was considered by some to be a national security issue. On steel, we would submit that the transaction was not a matter of national security because the proposed new owner of U.S. Steel came from a close ally of the United States, Japan, and since the proposed sale involved no change in the production's physical location.

The more recent discussion about the state of aluminum production can be viewed through a similar prism. While the United States has allowed its aluminum production capabilities to atrophy considerably in recent decades, much of that production is for goods of convenience—like soda and beer cans—not crucial national security platforms. Moreover, in an emergency, there are ways to build recycling facilities fairly fast that could considerably expand national capacity for new aluminum production.[14] Producing some aluminum in the United States may be wise, but we would argue that there is no national security imperative to onshore most of the U.S. supply of aluminum.

How can we scope this challenge systematically? A good starting point is provided by the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security. It has developed a list of 16 areas of critical infrastructure, defined as physical and virtual assets and systems so vital to the nation that their incapacity or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination thereof.[15] The 16 sectors are as follows:

- Chemicals.
- Commercial facilities.
- Communications.
- Critical manufacturing.
- Dams.
- Defense industrial base.
- Emergency services.
- Energy.
- Financial services.
- Food and agriculture.
- Government services and facilities.
- Health care and public health.
- Information technology.
- Nuclear reactors, materials, and waste.
- Transportation systems.
- Water and wastewater.

Which of these requires further examination to determine if there are supply chain vulnerabilities that could involve the potential for hostile foreign interference or some other potential single point of failure?

The framework we propose takes the 16 critical infrastructure sectors and asks the following questions to assess the relevance of their supply chains to national security:

1. To what extent does the sector rely on manufacturing supply chains for continued operations?
2. To what extent are these supply chains reliant on potentially adversarial nations?
3. In case of supply chain disruption, would significant harm result before supply chains could be replaced or restored?

We classify sectors as presenting acute national security supply chain concerns only when all three criteria apply strongly.

Applying the framework to critical infrastructure sectors

This section evaluates all 16 CISA-designated critical infrastructure sectors against our three-part framework: (1) reliance on supply chains for operations, (2) exposure of those supply chains to potentially adversarial nations, and (3) the speed and magnitude of harm if supply chains are disrupted. We begin by examining sectors where at least one criterion does not present significant concern, before moving to sectors where the analysis reveals more complex and layered vulnerabilities.

AREAS OF LITTLE APPARENT SUPPLY CHAIN CONCERN

At some risk of oversimplification, several categories of infrastructure do not seem likely to involve supply chain vulnerabilities. Some of these sectors may require protection against terrorism or other possible threats (human-made or natural), but not in a way that involves manufacturing supply chains.

Take **stadiums** and other large gathering sites, for example, which form a part of the commercial activities category on the list. These are places that can be attacked, causing a large loss of life and panic. While they should be considered critical infrastructure, they do not tend to involve technologies that are rare or difficult to reproduce. Some relevant equipment does come from China—large screen displays, seats, and sports equipment—but the larger point is that, even if the nation needed to make do without many such public gatherings for a period of months or even longer, the country's basic viability would not be at risk. Thus, sports-related equipment and materials used in constructing public gathering places do not belong in any parsimonious definition of the national security industrial base.

Or take **dams**. The main constituent elements are piping, concrete, and electrical equipment. Other relevant technologies include large turbines and transformers, as well as large components of turbines that must be cast. In other words, it is not the dams themselves so much as the associated hydroelectric systems that involve some foreign dependencies. Many of the foreign providers are friends, like Brazil and Canada, and much of the equipment required is in fact produced in the United States. The main specific technology where the United States might feel a strong impetus to boost domestic production capacity is with large hydrogenerators, given China's relatively important role in global production of these technologies. But even here, the timelines usually involved in replacing such equipment (years and decades), as well as the number of friendly suppliers, means the situation is not particularly acute.[16]

That said, since we know that China has sought to create the capability to sabotage U.S. infrastructure, possibly including dams, the United States should seek to avoid supply chain dependencies that would provide China or another potentially hostile foreign actor access to fragile parts of such critical infrastructure. This caution would not necessarily arise from concern that access to parts or components would be cut off in a crisis, but that malware within such elements of infrastructure that were already operational within the United States could be activated for nefarious purposes. There are certain types of technologies that should simply not be sourced from rivalrous foreign actors for this kind of reason, as the below discussions of cranes and electric vehicles reinforce.[17]

The **emergency services** sector is centered on vehicles that are produced in large numbers in the United States or could easily be produced here if necessary. Yes, the vehicles contain chips and other electronic components that the United States often sources from abroad, but in a crisis, the nation could give priority to the production of adequate numbers of emergency-sector vehicles even if that meant slowing other vehicle production. Thus, it is doubtful that vulnerable supply chain issues would arise in regard to this sector of critical technology (except with health care products and materials, discussed further below).

Financial services involve lots of computer technologies and must be protected against physical attack or cyberattack. The computer technologies of importance to this economic sector are addressed in a separate category below. Otherwise, some components for things like ATMs are produced abroad.[18] This situation does not strike us as a major national security problem; there are ways the country can make do with fewer ATMs for a time, for example. Thus, as with the other categories discussed above, the financial services sector of the economy does not seem to present specific vulnerabilities in the national security industrial base.

Similarly, **non-military government services**—covering administrative buildings, courthouses, schools, and government data and service centers—do rely on supply chains, but their day-to-day operations overwhelmingly depend on basic utility and service inputs: water, electricity, IT, communications, transportation, and maintenance supplies. Their unique supply chain dependencies are limited. They do source physical materials (office equipment, security tech, facility maintenance), but these are not distinct or mission-critical in the same way as defense or health care.

Water and wastewater treatment infrastructure, like dams, can be targeted by an adversary intent on hurting lots of people. For water and wastewater supply chains, there are some cases where specific technologies like control systems and membranes come from foreign suppliers, but most of the supplies and suppliers are from Europe, friendly countries in East Asia, and North America.[19] Some chemicals used in water treatment, especially chlorine as well as sulfur-based and phosphate-based chemicals, are largely sourced abroad, but again, the vulnerabilities seem modest, as most foreign sources are in the Western Hemisphere.[20] On balance, while there may be some modest exceptions, water and wastewater treatment infrastructure does not seem to display many vulnerabilities to an adversarial supply chain disruption. (It does, however, have cyber vulnerabilities due to malware that might be planted within it, as due to China's "Volt Typhoon" effort,[21] and this matter requires serious attention to improve cybersecurity even if it is not within our main purview here.)

INFRASTRUCTURE WITH POTENTIAL FOREIGN SUPPLY CHAIN VULNERABILITIES

This analysis leaves us with nine categories of critical infrastructure: agriculture, chemicals, energy, nuclear reactors, communications networks, transportation networks, health care, IT, and critical manufacturing. That latter category, according to CISA, comprises firms that produce primary metals, machinery, electrical equipment, and transportation products essential to the functioning of other critical infrastructure and the broader economy.

Since this is a preliminary scoping paper, we do not seek to be comprehensive or detailed in our analysis. Rather, we would offer several provisional observations about where vulnerabilities may exist and encourage the government, with its greater resources, to examine these areas of infrastructure in greater detail en route to developing an agenda for action and vulnerability mitigation.

Within the American **energy economy**, dependencies on potentially hostile foreign actors seem modest, with some limited exceptions. For example, China produces about a quarter of the world's supply of a substance known as barite, a component of drilling mud that is used to maintain correct wellbore pressure and prevent well blowouts.[22] Then there is the matter of supply chains for equipment in oil refineries, of which the United States now has about 130.[23] Most key machinery within them, including devices such as pumps, is not sourced from China or other potentially hostile single-point-of-failure countries.[24] Some of the chemical reagents and precursors used in oil refineries are, however, purchased in substantial amounts from China. These particular dependencies merit further scrutiny and, in some cases, consideration of either stockpiling or development of alternative sources of supply.

America's huge distribution system for natural gas and petroleum products includes millions of miles of **pipelines**, the operation of which requires a steady supply of valves, fittings, pipes, welding and corrosion control materials, inspection and cleaning devices, compressors, and control electronics.[25] Chinese components in these pipeline networks appear generally modest (and have already been curtailed somewhat by policy).[26]

The United States—like much of the rest of the world—has developed a dependency on China for solar panels. As a matter of competitiveness in an important technology, this is regrettable. However, it may not constitute a serious national security vulnerability per se.[27] Even if a supply disruption slowed the transition to solar energy (or electric vehicles), it would not bring the U.S. economy to its knees or directly threaten the safety of large numbers of Americans. This example highlights why not every instance of foreign dominance in advanced industry rises to the level of a national security threat.

In terms of energy transmission and electricity, China is the source of about 10% of U.S. high-power electrical transformers in the United States today—in and of itself, perhaps not an undue percentage.[28] Those transformers switch voltages of current, making them crucial nodes in the nation's electricity distribution system.

There are two types of supply chain concerns in regard to the sector in particular. One is that China could install software that gives it the ability to shut down or otherwise compromise the performance of those transformers; indeed, it appears to have done so already through the work of its Volt Typhoon group.[29] The second potential concern is that, should the United States need more transformers at a given moment and find other sourcing lacking, China might decline to provide replacements or to fill new orders especially in the context of a U.S.-China security crisis or conflict. Thus, while the United States' scale of dependency on China today is not enormous, there may be a case to reduce it further. The United States should also examine components of key technologies; it is entirely possible that China produces a larger share of certain components for transformers than of the finished goods themselves. That is a general cautionary note that applies to a number of the technologies we consider in this (scoping) paper, perhaps most notably in the pharmaceutical sector, as discussed further below.

For the most part, U.S.-based **nuclear reactors** do not incorporate much foreign technology except from suppliers in Japan, South Korea, and other friendly countries for large elements like steam generators and heavy castings.[30] Moreover, reactor construction and major renovation happen over time frames of years and decades, reducing the need for assured and constant access to crucial components (unlike the situation, say, with pharmaceuticals, as discussed below).

There is a major caveat to this conclusion: the United States is almost totally dependent on overseas providers for the uranium fuel used in these reactors (and to produce molybdenum-99, a key element in medical imaging machines). Specifically, about half of U.S. uranium concentrate (U_3O_8) imports comes from Canada and Australia; the other half comes from Kazakhstan, Uzbekistan, and Russia.[31] The situation is being partly remedied through recent government initiatives to beef up domestic enrichment capacity, and to require waivers for further imports from Russia.[32] Regardless, the problem may not be a top-tier national security concern; even if reactor operations in a worst case scenario had to be slowed somewhat, the country could continue to produce the vast preponderance of its electricity by other means, since nuclear power only accounts for 20% of American electricity production, and not all of it would be lost suddenly.[33]

In terms of **motor vehicles and aircraft**, the United States does import some equipment, but it also makes a great deal of its own. Those sources of foreign technology are largely friendly or nearby countries, too, notably Canada, Mexico, Germany, Great Britain, France, Japan, and South Korea.[34] Many U.S.-made cars do include Chinese parts, largely electronics systems, however. In some cases, it may make sense to diversify.[35] But cars generally last a long time, and carpooling can be a partial antidote to temporary shortages of new vehicles, in a crisis.

On balance, this sector does not seem to rise to a top-tier national security industrial base concern, in terms of potential supply chain disruption. As with electricity, however, relying on advanced Chinese components may raise some concerns about possible sabotage, for example, through "zero-day" malware that could in theory be activated in a crisis and disable a sizeable fraction of the U.S. automobile fleet. Since electric cars can be viewed as packages of mobile sensor systems and advanced computers linked to communications networks, there is a case to be made that Chinese or other potentially hostile foreign suppliers should simply not be allowed to sell such technology in the United States. Again, the concern is not the possibility of acute shortages due to an embargo, but vulnerability due to Chinese-made systems that are already in the United States and that could be gathering intelligence in peacetime or be activated by malware to malfunction in a time of crisis.

Other concerns about foreign supply chain dependency in the transportation sector relate to **ships and to port equipment**.[36] American commercial shipbuilding is very weak, meaning that the country cannot realistically build ships for its trade needs and must therefore rely on other nations. To the extent the latter includes close American allies, notably Japan and South Korea, the danger is modest, as noted before. But on balance, there is a compelling case, it would seem to us, for strengthening American shipbuilding through sustained government and private-sector effort. Notably, the U.S. Navy remains smaller than many would prefer due largely to supply chain constraints—and, therefore, its prospects for surging production in a protracted conflict would be unpromising.

Cranes for ports fall into the kind of category noted above for transformers. They may be too crucial to the economy's functioning for the country to tolerate the risk of malware being implanted in them by a hostile foreign actor, for possible activation during a crisis. Perhaps some types of trade are less sensitive and can be serviced with Chinese cranes as well as associated infrastructure, but the overall situation is very concerning, especially in regard to a Chinese company known as ZPMC, the world's largest producer of cranes, as its cranes have been found to contain unauthorized modems.[37] This issue does appear to be receiving attention of late, notably in the Select Committee on the Chinese Communist Party of the U.S. Congress, with the goals of better monitoring Chinese-sourced crane technologies and in some cases replacing them, but considerable additional remedial effort is still needed.[38]

On a final matter regarding transportation, **air traffic control** and management technologies are largely built by the United States as well as major European allies. This does not seem to be an area of major vulnerability in terms of supply chain interruptions.[39]

Thankfully, the United States makes many of its satellites and other core elements of the country's **telecommunications systems**, including undersea fiber-optic cables.[40] The nation has focused on keeping Huawei 5G out of the United States, has protected key national technology jewels through the Committee on Foreign Investment in the United States, and has recently undertaken several efforts to expand semiconductor chip production within the United States as well. With Huawei and other Chinese companies effectively shut out of the 5G cellphone network project in the United States, moreover, China or any other major potentially hostile foreign actor has limited inroads into the American hardware grids upon which communications systems depend.[41]

Then there is the question of the **phone** itself, where the world has developed a major dependency on China for assembly. Yet this may not be a serious supply-side vulnerability of a magnitude that should be viewed as a top-tier national security matter. Should China ever cut off exports in a crisis, some of the assembly capability could be recreated elsewhere within a time horizon that would probably allow for general connectivity to be sustained, given that phones generally can have up to several-year lifetimes.

In terms of **IT hardware**—basically, chips and things made from chips, as well as things like visual displays and printed circuit boards—a great deal of attention has already been paid to this subject in recent years. The CHIPS and Science Act of 2022 has helped catalyze the construction of numerous advanced microchip fabrication plants in the United States, and some are already in operation. There is a ways to go, however, and even where chipmaking plants are built on American soil, there can remain overseas dependencies on raw materials such as key chemicals in the production process (as we discuss further below).[42]

It should be noted that there are three distinct, if interrelated, aspects to **chip production** supply chain resilience and security. One is making sure that enough chips continue to reach the country to keep vital systems, including military hardware and critical infrastructure, functional. That is truly a national security imperative. A second is to be sure that those chips within weapons and critical infrastructure are reliable—that is, that they do not contain malware. Since most chips come from U.S. allies, this may not be a major concern, though it merits ongoing vigilance. A third is to ensure that enough chips remain available even in times of crisis to leave the broader consumer economy relatively unaffected. This last matter, while important, is arguably less crucial than the other two from a national security perspective. Given that under current projections the United States would garner more than 25% of the market share for advanced global chip manufacturing by 2032, the country seems headed in a sound direction, at least for advanced chips.[43] Further attention is still needed for other areas of potential vulnerability, however, such as the production of more basic chips and of certain other key electrical components.

The American **chemical sector** is vast. Not all areas appear to be of similar concern, however, in regard to dependencies on vulnerable overseas supply chains. There are specific foreign dependencies for chemical imports in the semiconductor industry, for example, including silicon, lithium, cobalt, fluorinated gases, and plastics. In these latter domains, the areas of greatest dependence on China include fluorides and some other gases needed in chip production, as well as silicon and other key ingredients in making batteries.[44] We would advise attention to this matter and perhaps an effort to further diversify supply.

In the realm of **agriculture**, responses to COVID-19 improved some types of redundancy and resilience, as in regard to regional hubs for food production.[45] But vulnerabilities remain. Some key chemicals, such as pesticides, are produced in large amounts in China, and that may constitute a vulnerability worthy of attention for certain specific chemicals. Fortunately, the dependencies on China are not overbearing, but are typically in the range of 10% to 20% of total U.S. needs. The overall sector involves annual trade measured in the hundreds of millions or low billions of dollars. It is worth bearing in mind too that, as with pharmaceuticals, China often produces precursor chemicals, so greater fidelity in trade statistics is needed to understand the full range of potential dependencies.[46]

In addition, some fertilizer used in American agriculture comes from Russia and Belarus. Again, as with chemicals, the proportionate dependency is modest, as Canada is the major foreign fertilizer supplier for the United States.[47] Also, in the event of a prolonged cutoff of key inputs to modern agriculture, some crop substitution may be possible. That may not be an ideal outcome for all farmers or consumers, but it could still reach the threshold for protecting national security.

The critical infrastructure in the **health care sector**—including hospitals, clinics, pharmacies, manufacturers, and distributors—is designed to deliver essential health services but depends heavily on the reliable supply of medicines and a range of medical devices.

The United States remains heavily reliant on China for **personal protective equipment** (PPE), with Chinese suppliers providing more than half

of all imported masks, gloves, and gowns in recent years. In response to critical shortages during the COVID-19 pandemic, the U.S. government has tried to lower this exposure by invoking the Defense Production Act, boosting domestic manufacturing capacity, and creating strategic national stockpiles, while some federal contracts now prioritize U.S.- or ally-made PPE. Despite these efforts, a substantial Chinese market share persists, and diversification has been slow, given persistent cost and supply advantages in China.

For **pharmaceutical products**, U.S. exposure to China is significant but concentrated in specific, critical areas of the supply chain. The more than 2,000 small-molecule drugs used in the United States[48]—whether chemically synthesized or fermented—each rely on multiple and varied upstream inputs for production. Reliance on China for finished drugs or their active pharmaceutical ingredients (APIs) is less pronounced than commonly assumed, but Chinese dominance is significant in the upstream stages: the key starting materials, intermediates, and auxiliary chemicals—such as reagents and solvents—that are essential for synthesizing APIs. China also controls critical intermediate production processes that have few viable alternatives, particularly for antibiotics, statins, and certain other therapeutic classes that depend on specialized synthesis steps like fluorination.[49]

Yet not all drugs and medical products rise to the national security level once we apply the framework criteria. For example, consider drugs that have intermediate manufacturing steps heavily reliant on China: statins through fluorination, and antibiotics and certain cancer drugs through fermentation.[50] Shortages of these drugs would have an adverse impact on patients; however, the time to harm and the time to recovery from a supply chain disruption differ substantially. The time to recovery is not immediate: even if there are alternative European suppliers (as there are for antibiotics[51]), switching suppliers would require establishing that products perform similarly with new inputs. In the meantime, the time to harm differs substantially for these drugs: it is immediate or rapidly detrimental for antibiotics and cancer drugs, whereas for statins, it is delayed and becomes clinically significant only after sustained interruption of therapy over months or years."[52]

This contrast underscores that what makes a health care product "national security critical" depends not on its complexity or prevalence alone, but on the degree and timing of harm if supply were to be disrupted—and how long it would realistically take to restore access through new manufacturing or alternative sourcing.[53]

The last segment we review is the **critical manufacturing sector** in the United States.[54] China is a major supplier to the United States in some categories of industrial equipment—boilers, motors, wiring, control systems, industrial machinery, HVAC systems, printed circuit boards, capacitors, and so on.[55] Some of these are not truly crucial, however—in the sense that even if supplies were interrupted for a time, the country's lifeblood would not be threatened. Notably, the production lines for most types of consumer durables should probably not be viewed as part of the national security industrial base. If the nation must make do without a steady supply of every type of major appliance, automobile, and the like for a time, it could presumably delay purchases, ration formally or informally, and tighten the collective belt for a period of time.[56]

In summary, this examination of 16 sectors of critical infrastructure in the United States leads us to underscore several categories of vulnerabilities requiring further attention and policy redress, primarily within 10 of the 16 infrastructure sectors (including the defense industrial base). There is good news; the number of such major categories of raw materials or supply chain components where acute shortages could quickly imperil American national security is not that large. But several issues do stand out:

Rare earth elements—including gadolinium, yttrium, and terbium—are essential to electricity grids, communications networks, defense systems, and advanced manufacturing. They are

also critical to health care: gadolinium is the key component of MRI contrast agents used in diagnostic imaging,[57] and rare earth elements are used in drug manufacturing catalysts and advanced diagnostic equipment. When China controls these materials' upstream processing, a disruption affects health care, energy, defense, and communications simultaneously. We realize that the U.S. political system has paid considerable attention to this issue of late. But the pace at which the country is mitigating its vulnerabilities seems far too slow (in contrast, for example, to the situation with semiconductors, where remedial action is happening faster).

Chemicals are another cross-cutting input essential to pharmaceutical manufacturing, water treatment, agriculture, energy infrastructure, and defense systems. In health care, small-molecule drugs are either fully or partially chemically synthesized, and medical devices require chemical coatings and sterilization agents. Water treatment depends on chlorine and caustic soda. Agriculture relies on fertilizers and pesticides. Energy infrastructure requires specialty chemicals for batteries and fuel additives. Defense manufacturing uses advanced coatings, composites, and specialized compounds for weapons systems. And China is a major producer of many such chemicals.

Critical infrastructure sectors also depend directly on each other. Hospitals cannot function without electricity, water, communications, and IT systems. Transportation networks depend on fuel and power. Water utilities require power for pumping. Financial systems rely on telecom and data processing. Disruption in one sector immediately degrades others—a hallmark of cascading failure risk. Because these overlapping nodes amplify systemic risk, their exposure should elevate the prioritization of sectors at the highest risk of cascading disruptions, making cross-sector resilience strategies especially urgent. China, in particular, is not a major supplier of key supply chain intermediate goods or finished products for most of these. Yet it does have some access to American infrastructure—in some cases, more than would be advisable.

Next steps: Refining prioritization and tool selection

While this paper proposes an initial framework for identifying supply chains critical to national security and vulnerable to adversarial disruption, the conversation is far from complete.

Implementing this framework requires clear assignment of institutional responsibility, rigorous selection of policy tools tailored to different vulnerabilities, and ongoing refinement as conditions evolve. The work ahead is to embed these processes into government routines and build the capacity—analytical, technical, and budgetary—to sustain them. We offer here a few initial thoughts designed to help spark a conversation about implementation strategies and methods.

REFINING PRIORITIZATION CRITERIA

Refining prioritization for physical supply chains requires three concrete steps. First, develop standardized, publicly available criteria incorporating these factors: exposure to China or other adversarial sources, time to harm if disruption occurs, and the feasibility of domestic or allied rebound (by creating substitution or alternative supply) before harm results. Second, ensure that prioritization incorporates lessons from previous crises (such as COVID-19, semiconductor shortages, and the embargoes of rare earth minerals in 2010, as well as more recently) and regularly updates risk assessments as conditions evolve. Third, institutionalize regular reviews using scenario-based stress tests and input from agencies, industry experts, and independent analysts.

SELECTING AND REFINING POLICY TOOLS

Selecting the right policy tools requires a rigorous, evidence-based approach. Agencies must assess which interventions—stockpiles, tax credits, subsidies, or regulatory measures—best fit the specific vulnerability, rather than defaulting to prior practices. Tools should be chosen for scalability, efficiency, and minimized unintended consequences. For example, strategic stockpiles suit high-value, durable goods but are impractical for bulk or fast-moving items, while competitive markets may benefit more from targeted subsidies than warehousing. Effective risk management relies on sectoral expertise paired with ongoing evaluation to prevent fragmentation and ensure interventions align with industry realities.

FEDERAL, STATE, AND LOCAL ROLES

National security supply chain policy is inherently a federal responsibility. The federal government possesses unique tools that state and local actors cannot deploy—selective regulation using trade policy, procurement mandates, or sectoral restrictions to shift supply chains away from adversarial nations where markets alone have failed. Federal investment in foundational research and development, coordination across sectors and regions, and strategic partnerships with allies also require centralized authority.

States and localities contribute significant value through on-the-ground execution, leveraging regional assets to develop clusters, build workforce capacity, and foster supplier networks. While federal action is crucial where vulnerabilities are most acute or industrial capacity is lacking, state-led efforts—supported by federal funding—enhance innovation and resilience by tailoring strategies to local strengths. Effective supply chain policy thus depends on rigorous evaluation, ensuring the right mix of federal leadership and state and local expertise for each sector's needs.

MAKING DE-RISKING EFFORTS SUSTAINABLE

The COVID-19 pandemic revealed that reactive measures—such as emergency stockpiling and short-term surges in production—are not enough to deliver lasting resilience. When immediate risks faded after the acute phase of the COVID-19 crisis, demand and prices crashed, causing new facilities to shutter and supply chains to return to pre-pandemic patterns dominated by low-cost offshore sourcing. Without reforms to reimbursement policies, procurement practices, and contract structures, many types of efforts wind up being temporary fixes that do not address the underlying market incentives driving vulnerability.

True sustainability in de-risking requires embedding resilience into normal operations through incentives for diversification, multiyear procurement commitments, and routine rotation of stockpiles. Firms and industries must be rewarded for maintaining backup suppliers, workforce capabilities, and domestic production capacity—so resilience becomes a permanent feature, not a crisis-driven exception. Only then will supply chains be able to adapt and withstand future disruptions, rather than reverting after each emergency.

Conclusion

Securing U.S. supply chains for national security requires not only clear criteria for what we protect but also disciplined choices about how to do so. It is also important to assess the proper roles of different actors and adjust when necessary; for example, the private sector can provide capital but may not always have the same incentives for improving resilience that must be the federal government's top priority. By embedding regular prioritization and rigorous tool selection into policy routines, the U.S. can safeguard the sectors that matter most—without succumbing to overreach or inefficiency. The work is ongoing, and structured adaptation is the best path to lasting resilience.

There is good news in our initial assessment. Yes, the United States has a number of previously unexplored and unrecognized vulnerabilities in global supply chains of relevance to national security. But the scope of the problem is not beyond our ability to comprehend and address, especially if we remain disciplined in determining what should count as a national security vulnerability and what should not. The nation's efforts of the past half dozen years or so to redress a number of existing vulnerabilities have already put us well on the path towards national resilience; now the challenge is to step back, take a broader look at the challenge, figure out what we have missed to date, and get after it.

Endnotes

1 Dexter Filkins, "Is the U.S. Ready for the Next War?" *The New Yorker*, July 14, 2025, https://www.newyorker.com/magazine/2025/07/21/is-the-us-ready-for-the-next-war.

2 "Securing Defense-Critical Supply Chains," (Washington, DC: Department of Defense, February 2022), https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF.

3 Ibid., 14.

4 "National Defense Industrial Strategy (Washington, DC: Department of Defense, November 2023), https://web.archive.org/web/20251004225408/https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf.

5 Luke A. Nicastro, "Implementing the National Defense Industrial Strategy: Issues for Congress," Congressional Research Service, November 2024, https://www.congress.gov/crs-product/IN12459; "National Defense Industrial Strategy Implementation Plan," (Washington, DC: Department of Defense, October 2024), https://www.govinfo.gov/content/pkg/GOVPUB-D-PURL-gpo234260/pdf/GOVPUB-D-PURL-gpo234260.pdf.

6 Hannah Miao, "Rare-Earth Magnet Maker Raises $65 Million in Push to Counter China," *The Wall Street Journal*, August 11, 2025, https://www.wsj.com/business/rare-earth-magnet-maker-raises-65-million-in-push-to-counter-china-85ea8612?mod=mhp.

7 William Booth and Laris Karklis, "Trump Covets Rare Earth Riches, But Greenland Plans to Mine Its Own Business," *The Washington Post*, July 27, 2025, https://www.washingtonpost.com/world/interactive/2025/greenland-minerals-mining-trump-difficulties/?itid=hp_mv-top-stories_world_p007_f001.

8 Elizabeth A. Holley and Priscilla P. Nelson, "Here's a Source for Critical Minerals—Hiding in Plain Sight," *The Washington Post*, September 1, 2025, https://www.washingtonpost.com/opinions/2025/09/01/critical-minerals-rare-earths-recovery/.

9 Ben A. Vagle and Stephen G. Brooks, *Command of Commerce: America's Enduring Economic Power Advantage over China* (Oxford: Oxford University Press, 2025), 125-128.

10 Greg Ip, "The U.S. Marches Toward State Capitalism with American Characteristics," *The Wall Street Journal*, August 11, 2025, https://www.wsj.com/economy/the-u-s-marches-toward-state-capitalism-with-american-characteristics-f75ca-fa8?mod=mhp.

11 See Mark Muro and Yang You, "The Nation's Advanced Industries Are Falling Behind, But Place-Based Strategies Can Help Them Catch Up," (Washington, DC: The Brookings Institution, September 7, 2023), https://www.brookings.edu/articles/the-nations-advanced-industries-are-falling-behind-but-place-based-strategies-can-help-them-catch-up/.

12 Marta E. Wosińska and Yihan Shi, "US Drug Supply Chain Exposure to China," The Brookings Institution, July 25, 2025, https://www.brookings.edu/articles/us-drug-supply-chain-exposure-to-china/.

13 "QuickStats: Percentage of Adults Aged ≥18 Years Who Took Prescription Medication During the Past 12 Months, by Sex and Age Group — National Health Interview Survey, United States, 2021," *MMWR: Morbidity and Mortality Weekly Report* 72, no. 16 (April 21, 2023): 451, https://www.cdc.gov/mmwr/volumes/72/wr/mm7216a7.htm.

14 Ryan Dezember, "America Doesn't Have an Aluminum Shortage. It's Just Sitting in Your Garbage," *The Wall Street Journal*, August 11, 2025, https://www.wsj.com/finance/commodities-futures/how-to-offset-trumps-aluminum-tariffs-recycle-your-beer-can-956cf433?mod=mhp.

15 "42 U.S. Code § 5195c - Critical Infrastructures Protection," Cornell Law School Legal Information Institute, accessed November 8, 2025, https://www.law.cornell.edu/uscode/text/42/5195c.

16 "Hydropower Supply Chain Gap Analysis," (Washington, DC: Department of Energy, August 2024), https://docs.nrel.gov/docs/fy24osti/88798.pdf.

17 Microsoft Threat Intelligence, "Volt Typhoon Targets U.S. Critical Infrastructure with Living-off-the-Land Techniques," Microsoft, May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

18 Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry," (Washington, DC: U.S. Department of Commerce and Department of Homeland Security, February 24, 2022), https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf.

19 See, for example, "Global Presence," Toray, 2025, https://www.water.toray/about/presence/.

20 "Understanding Water Treatment Chemical Supply Chains and the Risk of Disruption," (Washington, DC: Environmental Protection Agency, December 2022), https://www.epa.gov/system/files/documents/2023-03/Understanding%20Water%20Treatment%20Chemical%20Supply%20Chains%20and%20the%20Risk%20of%20Disruptions.pdf.

21 "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Cybersecurity and Infrastructure Security Agency, February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

22 "Mineral Commodity Summaries 2025," (Reston: U.S. Geological Survey, March 2025), https://www.usgs.gov/centers/national-minerals-information-center/mineral-commodity-summaries.

23 "Petroleum & Other Liquids," U.S. Energy Information Administration, June 6, 2025, https://www.eia.gov/dnav/pet/hist/LeafHandler.ashx?f=A&n=PET&s=8_NA_8O0_NUS_C.

24 "Air or vacuum pumps, air or other gas compressors and fans; ventilating or recycling hoods incorporating a fan, whether or not fitted with filters | Value (US$) and Value Growth, YoY (%) | 2012 - 2023," TrendEconomy, January 2024, https://trendeconomy.com/data/h2/UnitedStatesOfAmerica/8414.

25 "Natural Gas Explained: Natural Gas Pipelines," U.S. Energy Information Administration, last updated March 19, 2024, https://www.eia.gov/energyexplained/natural-gas/natural-gas-pipelines.php.

26 Klaus Brun, "The US Natural Gas Compression Infrastructure: Opportunities for Efficiency Improvements," Elliott Group, October 2018, https://netl.doe.gov/sites/default/files/netl-file/Brun.pdf.

27 "Summer 2024 Solar Industry Update," (Washington, DC: Department of Energy, 2024), https://docs.nrel.gov/docs/fy24osti/91209.pdf?utm_source=chatgpt.com.

28 Justin Sherman and Tianjiu Zuo, "Energy Grid Supply-Chain Risks and U.S.-China Entanglement," Lawfare, June 8, 2020, https://www.lawfaremedia.org/article/energy-grid-supply-chain-risks-and-us-china-entanglement#:~:text=In%20the%20past%20decade%2C%20China,the%20same%20volume%20as%20China.

29 Anne Neuberger, "China Is Winning the Cyberwar: America Needs a New Strategy of Deterrence," *Foreign Affairs*, August 13, 2025, https://www.foreignaffairs.com/china/china-winning-cyberwar-artificial-intelligence; "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure."

30 "Heavy Manufacturing of Power Plants," World Nuclear Association, March 2021, https://world-nuclear.org/information-library/nuclear-fuel-cycle/nuclear-power-reactors/heavy-manufacturing-of-power-plants.

31 Slade Johnson, "U.S. Nuclear Generators Import Nearly All the Uranium Concentrate They Use," U.S. Energy Information Administration, January 30, 2025, https://www.eia.gov/todayinenergy/detail.php?id=64444#:~:text=Imports%20accounted%20for%2099%25%20of,U.S.%20nuclear%20fuel%20supply%20chain.

32 Rowen Price, "Nuclear Fuel 101: Front-End Processes, Prospects, and Policy," Third Way, March 27, 2024, https://www.thirdway.org/blog/nuclear-fuel-101-front-end-processes-prospects-and-policy; Parker Kleinman, "Breaking the Chain: Addressing America's Nuclear Fuel Dependency for an Advanced Energy Future," Nuclear Insider, January 21, 2025, https://nuclearinsider.com/breaking-the-chain-addressing-americas-nuclear-fuel-dependency-for-an-advanced-energy-future/.

33 "Electricity Data Browser," U.S. Energy Information Administration, August 2025, https://www.eia.gov/electricity/data/browser/.

34 "Transportation Equipment," United States International Trade Commission, 2022, https://www.usitc.gov/research_and_analysis/tradeshifts/2021/transportation#:~:text=The%20value%20of%20U.S.%20general,decreases%20from%20Canada%20and%20Singapore.

35 Michael Mariani, "Just How Dependent Is the Automotive Industry on Electronic Components Manufactured in China?" Z2Data, April 23, 2025, https://www.z2data.com/insights/how-dependent-automotive-industry-on-electronic-components-manufactured-china.

36 "U.S. Department of Transportation Marks Significant Progress on Efforts to Shore up Key Supply Chains and Lays Out Recommendations for Continued Success," U.S. Department of Transportation, December 19, 2024, https://www.transportation.gov/briefing-room/us-department-transportation-marks-significant-progress-efforts-shore-key-supply.

37 Carter Evans and Paul Facey, "Chinese Cranes at U.S. Ports Raise Homeland Security Concerns," CBS News, February 11, 2025, https://www.cbsnews.com/news/chinese-cranes-at-u-s-ports-raise-homeland-security-concerns/.

38 "Handling Our Cargo: How the People's Republic of China Invests Strategically in the U.S. Maritime Industry," (Washington, DC: House Select Committee on the Chinese Communist Party, September 2024), https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Joint%20Homeland-China%20Select%20Port%20Security%20Report-compressed.pdf.

39 Aashish Mehra, "Air Traffic Control Companies," Markets and Markets, 2025, https://www.marketsandmarkets.com/ResearchInsight/air-traffic-control-equipment-market.asp.

40 See Joe Brock, "Inside the Subsea Cable Firm Secretly Helping America Take on China," Reuters, July 6, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-subcom/.

41 "Information and Communications Technology Supply Chain Risk Management," Cybersecurity and Infrastructure Security Agency, 2023, https://www.cisa.gov/information-and-communications-technology-supply-chain-risk-management.

42 Chris Musso et al., "Creating a Thriving U.S. Chemical Semiconductor Supply Chain in America," McKinsey and Company, March 25, 2025, https://www.mckinsey.com/industries/chemicals/our-insights/creating-a-thriving-chemical-semiconductor-supply-chain-in-america.

43 "America Projected to Triple Semiconductor Manufacturing Capacity by 2032, the Largest Rate of Growth in the World," Semiconductor Industry Association, May 8, 2024, https://www.semiconductors.org/america-projected-to-triple-semiconductor-manufacturing-capacity-by-2032-the-largest-rate-of-growth-in-the-world.

44 "Chemicals and Related Products," United States International Trade Commission, 2020, https://www.usitc.gov/research_and_analysis/trade_shifts_2019/chemicals.htm.

45 Sabrina Halvorson, "USDA Works to Strengthen Food Supply Chain," Southeast AgNet Radio Network, January 9, 2025, https://southeastagnet.com/2025/01/09/usda-works-strengthen-food-supply-chain/.

46 Jim DeLisi, "Quick Look at Agrochemical Trade in the United States," Agribusiness Global, August 2023, https://www.agribusinessglobal.com/special-sections/quick-look-at-agrochemical-trade-in-the-united-states; Mickey Shan, "Interview | China-U.S. Pesticide Trade Relations: Navigating Complexity in Search of New Opportunities," Agnews, March 12, 2025, https://news.agropages.com/News/NewsDetail---53262.htm.

47 See Corey Rosenbusch, "TFI's Rosenbusch Testifies to Congress on Critical Nature of Phosphate, Potash," The Fertilizer Institute, June 4, 2024, https://www.tfi.org/media-center/2024/06/04/tfis-rosenbusch-testifies-to-congress-on-critical-nature-of-phosphate-potash; Henriqu Monaco, Gary Schnitkey, and Nick Paulson, "U.S. Fertilizer Industry in Global Markets: Structure and Supply Risks," Farmdoc Daily, July 29, 2025, https://farmdocdaily.illinois.edu/2025/07/us-fertilizer-industry-in-global-markets-structure-and-supply-risks.html.

48 "Statistics," DrugBank, accessed November 8, 2025, https://go.drugbank.com/stats.

49 Wosińska and Shi, "US Drug Supply Chain Exposure to China."

50 Ibid.

51 See comments by Jonathan Kimball, Sandoz, at the October 2025 National Academy workshop: "Improving Resiliency in the U.S. Pharmaceutical Supply Chain Through Make-Buy-Invest Strategic Actions: A Workshop," National Academies of Sciences, Engineering, and Medicine, October 22-23, 2025, https://www.nationalacademies.org/projects/PGA-GLOBAL-25-03/event/45111.

52 Lindsey C. Yourman et al., "Evaluation of Time to Benefit of Statins for the Primary Prevention of Cardiovascular Events in Adults Aged 50 to 75 Years," *JAMA Internal Medicine* 181, no. 2 (Nov. 16, 2020): 179-185, https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2773065.

53 Marta Wosińska, "What Policymakers Need to Know About China's Role in US Drug Supply Chains and What to Do About It," The Brookings Institution, September 17, 2025, https://www.brookings.edu/articles/what-policymakers-need-to-know-about-chinas-role-in-the-us-drug-supply-chains-and-what-to-do-about-it/.

54 Cyrille Schwellnus et al., "Global Value Chain Dependencies Under the Magnifying Glass," OECD Science, Technology and Industry Policy Papers, no. 142, https://doi.org/10.1787/b2489065-en; Vagle and Brooks, *Command of Commerce*, 145.

55 "United States Imports from China of Machinery, nuclear reactors, boilers," Trading Economics, 2025, https://tradingeconomics.com/united-states/imports/china/nuclear-reactors-boilers-machinery.

56 "Analysis of U.S. Trade with China, 2022," (Washington, DC: Department of Commerce, 2023), https://www.bis.doc.gov/index.php/documents/technology-evaluation/ote-data-portal/country-analysis/3420-2022-statistical-analysis-of-us-trade-with-china/file.

57 Michael A. Ibrahim, Bita Hazhirkarzar, and Arthur B. Dublin, "Gadolinium Magnetic Resonance Imaging," StatPearls, last updated July 3, 2023, https://www.ncbi.nlm.nih.gov/books/NBK482487/.

About the authors

Michael E. O'Hanlon is the inaugural holder of the Philip H. Knight Chair in Defense and Strategy and director of research in the Foreign Policy program at the Brookings Institution, where he specializes in U.S. defense strategy and budgets, the use of military force, and American national security policy. He is a senior fellow and directs the Strobe Talbott Center on Security, Strategy, and Technology.

Marta E. Wosińska is Ph.D., is a senior fellow at the Center on Health Policy at the Brookings Institution, where she specializes in the economics of prescription drugs, including supply chain issues.

Mark Muro is senior fellow at Brookings Metro, focusing on the interplay of technology, people, and place as they are altered by positive and negative disruptions.

Thomas (Tom) Wright is a senior fellow with the Strobe Talbott Center for Security, Strategy and Technology at the Brookings Institution.

Acknowledgments

The authors are grateful to Alejandra Rocha and Monica Gorman for their helpful comments and feedback on this paper. Special thanks are also due to Adam Lammon for editorial support and Rachel Slattery for layout support.

Disclaimer

This project is sponsored in part by the Uniformed Services University of the Health Sciences (USU); however, the information or content and conclusions do not necessarily represent the official position or policy of, nor should any official endorsement be inferred on the part of, USU, the Department of Defense, or the U.S. government.

BROOKINGS

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, D.C. 20036
brookings.edu