

Unraveling the Gordian Knot

Considering Supply Chain Resiliency

Caolionn O'Connell

CT-A1774-1

Testimony presented before the House Energy and Commerce Committee, Subcommittee on Consumer Protection and Commerce on October 14, 2021.



For more information on this publication,
visit www.rand.org/pubs/testimonies/CTA1774-1.html.

Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.

© Copyright 2021 RAND Corporation

RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.html.

Unraveling the Gordian Knot: Considering Supply Chain Resiliency

Testimony of Caolionn O’Connell¹
The RAND Corporation²

Before the Committee on Energy and Commerce
Subcommittee on Consumer Protection and Commerce
United States House of Representatives

October 14, 2021

The convergence of strategic, technological, economic, and industrial processes and systems in today’s era presents a unique challenge for supply chain resiliency. Supply chains have become a key part of broader national security considerations because they exhibit nothing less than the ability to engage in strategic competition in a highly interconnected world. Supply chain vulnerabilities are not confined to microchips and medical equipment; if we learned anything from the COVID-19 pandemic, it is that these global supply chains are often opaque to private and public decisionmakers. In this testimony, I will detail the breadth of the problem and the various roles the private and public sectors can have in increasing resiliency.

Breadth of the Problem

What Is a Supply Chain, and What Does Resiliency Mean?

A supply chain is the network of organizations—be they military, government, or private sector—involved in creating and delivering a product or service to a customer or consumer. The supply chain for a single complex product has frequently been referred to as a Gordian knot—so

¹ The opinions and conclusions expressed in this testimony are the author’s alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

² The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND’s mission is enabled through its core values of quality and objectivity and its commitment to integrity and ethical behavior. RAND subjects its research publications to a robust and exacting quality-assurance process; avoids financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursues transparency through the open publication of research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. This testimony is not a research publication, but witnesses affiliated with RAND routinely draw on relevant research conducted in the organization.

large and complicated that simply understanding all the links that compose a single supply chain can be an intractable problem.

Additionally, the scope of a supply chain should be interpreted more broadly to reflect dependencies on software. In the past, a *supply chain* has been defined as the raw materials and components required to manufacture a product. Although that definition will remain, it is grossly incomplete in modern-day society. We are quickly entering a world where cyber disruptions easily become supply chain disruptions and where supply chains for hardware and software create new cyber risks. In the production of programmable integrated circuits, the supply chain should include not only the chip designer and silicon foundry but also their software tools and the software tools used in programming and maintenance. Similarly, software installed to automate traditional manufacturing facilities may also be relevant and critical to a supply chain.

A resilient supply chain is one that can react quickly and efficiently to disruptions occurring within the network and continue to deliver the required good or service. In today's globalized economy, it is neither feasible nor desirable to return all production to the United States and eliminate all foreign sources from U.S. supply chains in an attempt to increase resiliency. In addition to the fact that it would be economically challenging to move all production to domestic sources, foreign sourcing can help mitigate some forms of supply chain risk. For example, when U.S. sources face disruptions from natural disasters, the ability to turn to foreign alternatives to reduce the risk of disrupted supply is invaluable. Given the inevitable exposure of U.S. supply chains to foreign countries and the benefits of accessing foreign sources of supply, the United States must consider carefully how much federal intervention is needed to ensure supply chain resilience and what portions of the supply chain merit that attention. Stimulating the manufacturing sector may well be a worthwhile investment, but, in and of itself, would be insufficient to ensure the resiliency and security of the U.S. supply chain without understanding which aspects of the manufacturing sector need that targeted assistance.

What Happens When Supply Chains Are Not Resilient?

The COVID-19 pandemic laid bare the fragility of global supply chains. As consumers, we remember shelves empty of toilet paper and long lead times for anything related to home improvement, but these are merely inconveniences when compared with the initial shortages for personal protective equipment for healthcare workers and ventilators.³

Software supply chains may be less vulnerable to natural disaster or pandemics, but they have become an important aspect of supply chains nonetheless. Using the SolarWinds hack as an example, hackers—suspected to be associated with Russia—added malicious code into SolarWinds' software system called Orion, which is used widely to manage information technology (IT) resources.⁴ The malware allowed attackers to compromise the servers on which

³ Jennifer Cohen and Yana van der Meulen Rodgers, "Contributing Factors to Personal Protective Equipment Shortages During the COVID-19 Pandemic," *Preventive Medicine*, Vol. 141, 2020, article 106263; and U.S. Food and Drug Administration, "Medical Device Shortages During the COVID-19 Public Health Emergency," September 10, 2021.

⁴ Joseph Menn and Christopher Bing, "Hackers of SolarWinds Stole Data on U.S. Sanctions Policy, Intelligence Probes," Reuters, October 8, 2021.

the Orion products run. About 18,000 SolarWinds customers, including multiple U.S. government agencies, were exposed to the vulnerability, thereby allowing hackers untold access to sensitive and proprietary information.⁵ SolarWinds is one supplier, and Orion is a single element in the IT supply chain. But one hack at the base of the supply chain exposed untold higher-level assets further up the tool chain. In a very real sense, an IT system is only as secure as the least secure piece of software that runs on the system, including the pieces of software used to design, build, and configure it.

How Much Do We Know About Supply Chains?

The federal government's key source of insight into its supply chains is the System for Award Management, which registers all of the prime, or Tier 1, contractors that do business with the federal government. Those businesses must provide information on their annual revenue, number of employees, and the industries in which they provide goods and services. The Federal Funding Accountability and Transparency Act Subaward Reporting System provides some Tier 2 supplier information (e.g., the subcontractors that the prime contractor engages), but it includes only subawards that are greater than \$25,000.⁶ This relatively high threshold means that a portion of the Tier 2 supply chain is not being captured. Given these limitations, U.S. government acquisition professionals have incomplete insight into their own supply chains unless they specifically request this information in contracts. In turn, a contractor can report only what it knows, and commercial firms often have little insight into businesses that are more than two tiers down from themselves.

These systems and complexities are related to just the federal government's supply chain, so consider the breadth of information required to understand the supply chains that underpin the U.S. economy and society. A U.S. regulation—Statement of Financial Accounting Standards No. 131—requires publicly traded firms to report all key customers that account for more than 10 percent of their total sales. This information is available in annual 10-K filings registered with the U.S. Securities and Exchange Commission, but in 2020, only 7,413 companies met the criteria that necessitate disclosing this information.⁷ According to U.S. Census data from 2018, there are more than 650,000 firms that employ at least 20 people in the United States.⁸ This means that slightly more than 1 percent of employers in the United States are required to disclose supply chain relationships—and only when that relationship crosses a significant threshold. For many companies, supplier information is considered proprietary. Only when information is reported in press releases or in government documents can relationships be inferred. In fact, there

⁵ U.S. Securities and Exchange Commission, SolarWinds Corporation, Form 8-K, December 14, 2020.

⁶ Nancy Y. Moore, Clifford A. Grammich, and Judith D. Mele, *Findings from Existing Data on the Department of Defense Industrial Base*, Santa Monica, Calif.: RAND Corporation, RR-614-OSD, 2014, www.rand.org/t/RR614.

⁷ Data from U.S. Securities and Exchange Commission, Electronic Data Gathering, Analysis, and Retrieval system, web tool, undated, <https://www.sec.gov/edgar>.

⁸ U.S. Census Bureau, “2018 SUSB Annual Datasets by Establishment Industry,” web tool, May 2021, <https://www.census.gov/data/datasets/2018/econ/susb/2018-susb.html>.

is a whole industry devoted to understanding these relationships and selling that information for a hefty licensing fee.

Increasing Supply Chain Resiliency

Role of the Private Sector

There is rich body of literature regarding best practices for commercial supply chain risk management. Two key metrics help businesses evaluate their risk exposure and right-size a resiliency strategy: The time-to-survive metric captures how long a business can continue if its supply chain is disrupted, and the time-to-recover metric captures how long it might take to pivot to another supplier. However, there is an implicit cost to ensure supply chain resiliency, and businesses will make those investments only if the perceived benefits outweigh the known costs.⁹

Role of the Public Sector

Put simply, one role of the public sector is to provide resources when market forces do not result in desired outcomes. In this context, the public sector may shore up vulnerable supply chains that support critical national security functions and essential elements of the U.S. economy for which the private sector has an incomplete appreciation of the risk or for which the cost burden outweighs the perceived benefits.

Market forces often generate local optimizations that do not consider the problem as a whole. For example, the supply chain for joint operations serves a joint force. However, the military services, geographic combatant commanders, the Defense Logistics Agency, and other combat support agencies make independent decisions about the purchase and positioning of spare parts and ordnance. These organizations have different responsibilities, authorities, and incentives that drive their supply chain decisions, which are optimized for the individual organizations. In practice, these competing priorities can reduce the overall effectiveness of the joint operating force that the organizations support. The public sector's role can be to make investments to increase the overall effectiveness.

Examples of Success

Perhaps there are lessons to be learned from Germany's approach to its manufacturing sector, which has an "independent nongovernmental organization that provides high-quality, short-term, affordable applied research that small and medium-size firms could not otherwise afford."¹⁰ Many German small and medium-sized enterprises dominate in niche markets because the superior quality and performance of their products allows them to command premium prices. But this model has been criticized for focusing on incremental improvements and stifling innovation.

⁹ David Simchi-Levi, William Schmidt, Yehua Wei, Peter Yun Zhang, Keith Combs, Yao Ge, Oleg Gusikhin, Michael Sander, and Don Zhang, "Identifying Risks and Mitigating Disruptions in the Automotive Supply Chain," *Interfaces*, Vol. 45, No. 5, October 2015, pp. 375–390.

¹⁰ Charles W. Wessner, "How Does Germany Do It?" American Society of Mechanical Engineers, November 13, 2013.

Similarly, although mainland China’s more centralized control of the economy is by no means mirrored in the United States nor a desirable goal, some lessons might be observed from China’s strategic approach to rare earth elements (REEs), which relied on export controls and investment in research and development to assume a dominant position in the global marketplace. REEs are raw materials that are essential to everything from electronic devices to wind turbines. In the mid-1980s, China overtook the United States in production partly because of the Chinese government’s consistent investment in REE-related refining and processing technologies and the U.S. desire to offshore the pollution caused by related mining and processing.¹¹ REEs became a protected strategic sector in China in the 1990s when the government issued a complete ban on foreign investment in mining REEs. In the 2000s, China began to move up the REE value chain by increasing the number of export restrictions (e.g., quotas and tariffs), which provided a powerful incentive for manufacturers that rely on REE to relocate their production facilities to China.¹² In 2019, China accounted for more than 65 percent of REE production.

Suggested Next Steps and Approaches

If, as the 2021 Executive Order on America’s Supply Chains states, the “United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security,”¹³ then the U.S. government must make the investments necessary to ensure that outcome, and businesses cannot be expected to shoulder the burden of this task without recompense.

Given the breadth of the problem, the solution requires a whole-of-government approach. The solution is likely multi-faceted and will need to include direct financial assistance to businesses deemed essential to bolstering resiliency; research and development dollars for innovation; and investment in human capital, such as vocational schools.

Research is necessary to determine which aspects of the supply chain pose an existential risk to the U.S. economy or the well-being of U.S. citizens. Initial work is underway,¹⁴ but there is still significant analysis to be done. No action should be undertaken without a relatively complete understanding of causes and consequences. Just as businesses must weigh the costs and benefits of supply chain resiliency, the U.S. government needs to understand the value

¹¹ Carlos Aguiar de Medeiros and Nicholas M. Trebat, “Transforming Natural Resources into Industrial Advantage: The Case of China’s Rare Earths Industry,” *Brazilian Journal of Political Economy*, Vol. 37, No. 3, July–September 2017.

¹² Richard Silbergliitt, James T. Bartis, Brian G. Chow, David L. An, and Kyle Brady, *Critical Materials: Present Danger to U.S. Manufacturing*, Santa Monica, Calif.: RAND Corporation, RR-133-NIC, 2013, www.rand.org/t/RR133.

¹³ White House, Executive Order on America’s Supply Chains, Washington, D.C., February 24, 2021.

¹⁴ Jonathan Welburn, Aaron Strong, Florentine Eloundou Nekoul, Justin Grana, Krystyna Marcinek, Osonde A. Osoba, Nirabh Koirala, and Claude Messan Setodji, *Systemic Risk in the Broad Economy: Interfirm Networks and Shocks in the U.S. Economy*, Santa Monica, Calif.: RAND Corporation, RR-4185-RC, 2020, www.rand.org/t/RR4185.

proposition of supply chain resiliency. Not all supply chains merit a federal intervention and, for sectors that are not essential, market forces should prevail.

Supply chain issues have finally come to the fore. This is, I hope, one of many conversations in this important dialogue that is so critical to national security and to the U.S. economy more broadly. Thank you for inviting me to appear before you today, and I look forward to answering your questions.