Chapter Three

Supply Chain

INTRODUCTION

During the last three years, a perfect storm of natural and geopolitical events has disrupted worldwide supply chains in ways that few governments could have anticipated. Even as nations, businesses, and consumers strive to normalize, new interruptions have created bottlenecks in an enormously complicated and interconnected system of purchasing, operation, distribution, integration, and consumption.

This chapter explores the role governments play in preparing for supply chain disruptions. It assesses how governments can foresee potential challenges, plan responses ahead of time, and be ready to minimize the impacts of supply chain disruptions. It outlines insights and recommendations on how best to diagnose threats, design responses, sustain supply chains, and mitigate disruptions by building supply chain immunity.

Setting the Context

In a 2022 survey, 38 percent of global CEOs reported that supply chain disruption is one of their greatest challenges.[1] And now, the impact of supply chain disruptions on national economies and social systems is driving government leaders to also put a top priority on building supply chain resiliency.

In the U.S., disaster and emergency events have typically been regional and limited in duration; examples include hurricanes, floods, fires, earthquakes, industrial accidents, or terrorist attacks. In all such cases, events generally evoked immediate action from emergency responders. The response to large scale disasters typically involves distribution of critical medical and disaster response supplies to surrounding regions, often following an established procedure for procuring and distributing supplies (e.g., food, shelter, water, and relief goods). Supplies are normally readily available, and past disaster response efforts have involved few problems in identifying qualified local suppliers for immediate contracting, acquisition, and shipping to impacted sites.

The COVID-19 pandemic was dramatically different. The national response infrastructure has never encountered an emergency where every industry sector was affected by disruptions at the same time. Government agencies were unfamiliar with how to address a disaster of this magnitude, which impacted every state in the country, every industry, every population, every hospital. The pandemic revealed significant gaps in the government's response capacity to this crisis, and response efforts have been the subject of many task forces and inquiries.

Source: The IBM Center report, Preparing Governments for Future Shocks: Collaborating to Build Resilient Supply Chains *by Professor Robert Handfield, North Carolina State University—as well as informed by the Future Shock Roundtable discussion and resources.*

The president's FY2023 budget request to Congress focused significant attention and investment proposals on strengthening supply chain operations and improving supply chain risk management and resiliency. The execution of these programs can be transformed by leveraging a "whole of government" scope and industry-leading supply chain management and shared services business models to their delivery. The box below highlights leading supply chain practices.

Current Leading Practices in Supply Chain Resilience and Preparedness

Digital transformation across interconnected processes and extended ecosystems with the expansion of new automation technologies provides predictability, flexibility, and intelligence to operations—especially in the automating of decision making. AI and intelligent, automated workflows can deliver 360-degree insights and impact analysis that provide this interconnectivity and optimize predictability. These workflows can benefit the workforce—digital and human—to dynamically adjust to the unforeseen with both self-learning and self-calibration.

With digital transformation comes increased vulnerabilities and security concerns for supply chains, including critical infrastructure, which is essential for supply chain performance. Additionally, there is an escalating need for visibility into who are comprising supply chain networks as well as transparency, providing that knowledge to external stakeholders. Leveraging digital transformation and intelligent workflows can address security concerns and make this visibility possible.

Current leading practices

As organizations implement technology into their supply chain practices, the following actions can help in their digital transformation:

- Use AI and machine learning to guide the quality and track performance of workflow reactions and decisions, as well as to monitor physical assets with predictability.
- Digitize to develop agile workflows to react quickly to escalating situations.
- Begin experimenting with quantum computing tools and methods to lay the groundwork for expanded capabilities.
- Combine predictive and prescriptive analysis for better decision making, while focusing on micro-insights revealed through extreme digitalization.

Current Leading Practices in Supply Chain Diversification

By its very definition, a chain is a series of entities linked, connected, or associated together. Extending that concept, a modern supply chain connects the organizations, activities, people, information, and resources that intersect to move products and services from producers to suppliers to end consumption—and now, with a focus on circularity, back again. These ecosystems are complex, interconnected, and global. They are ecosystems of partners, infrastructure, and resources.

Many organizations are investing in regionalization and localization strategies of product supply and production to decrease the risk of overreliance on a single region. Many are parsing the supply chain by segment to promote tighter collaboration with suppliers and service providers that have differentiated skills and capabilities—adding AI and algorithmic insights for increased risk management and predictive event forecasting.

Current Leading Practices

To be successful, modern supply chains operate through an ecosystem of partners and actions, outlined below, that can enable an organization to diversify their supply chain models:

- Use segmentation techniques to examine ecosystems in minute detail for increased collaborative opportunities across workflows with data-infused intelligent decision and action.
- Increase visibility and security in every touchpoint of supply chain workflows with extended ecosystems and partners.
- Reevaluate supplier networks with n-tier visibility and trusted data-sharing.

Current Leading Practices in Supply Chain Operations and Sustainability

An emerging perspective among forward-thinking leaders is that open innovation with business partners drives sustainability initiatives and transformation. In fact, many are finding a stronger alignment between their sustainability strategies and digital transformation initiatives.

Leaders from both public and private sectors are focused on improving energy efficiency, water management, and using more organic and recyclable materials—reporting that these sustainability initiatives will substantially change their supply chain models over the next two to three years.

Workflow digitization also contributes to helping organizations meet their sustainability objectives. As teams evaluate and build intelligent workflows, they can incorporate ways to reduce their environmental impact and move toward comprehensive circularity programs. In these programs, end-of-life products are not disposed of, they flow back into the supply chain.

Current Leading Practices

Sustainability initiatives are growing in importance within all facets of an organization's operations—including its supply chain model. The following actions can help with the integration of sustainability and supply chain operations:

- Optimize workflows with AI, automation, and virtualization to manage carbon, waste, energy, and water consumption.
- Use virtualization to help shrink environmental footprints and support the nine R's of circularity: Recycle, Reduce, Reuse, Repair, Refurbish, Remanufacture, Repurpose, Recover, Refuse.
- Experiment with open innovation and scientific discovery to explore future solutions and possibilities.

Insights and Recommendations

What is the role of governments in preparing for supply chain disruptions that impact government services, national defense, and national economies? How can governments foresee potential challenges, plan responses ahead of time, and be ready to minimize the impacts?

Insights from the Future Shocks roundtables and related research suggest that governments can establish a shared service center of excellence to develop protection against supply chain disruptions. After establishing these supply chain risk management organizations, governments should have the centralized resources to diagnose threats, design responses, sustain supply chains, and mitigate disruptions by building supply chain immunity.[2]

Create a shared service approach to build supply chain resiliency

Many disruptive scenarios require different responses from multiple government entities. This leads to a clear conclusion: to garner multiagency support and cross-sector collaboration for quick response, a shared service strategy can be a key form of engagement to build supply chain resiliency.

A shared service approach for supply chains would also incorporate a "center of excellence" (COE) model. A COE would consist of multiple agencies, and could include a data center with key information, predictive modeling capabilities, and an effective vendor-managed inventory. A multiagency shared service, with full-time subject matter experts contributing unique expertise and perspectives on supply chain disruption events. This team could also build out diagnostic data and organize more predictive models as foundations for "future state" planning scenarios.

However, managing a shared service is no easy task. Overseeing such an enterprise requires managing experts from multiple government agencies. A COE of this composition should also include leaders from the private sector to help ensure that the right channels are used for driving policies and implementation.

Research shows that the most critical components for building supply chain resiliency include:

- Real-time access to data on disruption effects
- Supply market intelligence with insights into mitigative actions
- Access to skilled experts who know what to do with this information

To strengthen the effectiveness and security of supply chains, agencies need to quickly execute decisions that drive actions, with a direct line to the right actors in each link of the supply chain. Developing these capabilities requires a combination of appropriate skills, supply risk technology, and communication channels that enable agile responses. Effective preparation cannot be taken for granted; supply chain readiness requires a defined process and a governance framework to analyze and respond, often based on limited options.

For these reasons, government-led, industry-involved shared service entity represents the most effective instrument for delivering capabilities to manage supply chain resilience.

ACTION STEPS

- By taking advantage of synergies between agencies and industry partners, a government-led shared service center of excellence can foster public-private collaboration to diagnose, design, and sustain supply chains to build resiliency.

Diagnose the acquisition ecosystem

Governments should begin by diagnosing the entire acquisition ecosystem and identifying key vulnerabilities, critical supply risks, and suppliers impacted by these risks. This takes considerable time and effort, given the difficulties involved with managing diagnostic work among multiple agencies and numerous businesses, trade associations, and international partners.

Vulnerability and risk may be further complicated by context. For example, a life sciences manufacturer described how chip shortages and the low availability of reagents impacted the provision of COVID-19 tests. In terms of national security, vulnerability means understanding the nature of component shortages. One defense industry expert explained, "The Tier 1 supplier was not the problem. The issue was a Tier 4 and a Tier 5 connector that was not available. The lack of one inexpensive part prevented more than a dozen aircraft from being deployed."

A June 2021 report[3] issued by the White House identifies four major supply chains as especially vulnerable:

- Semiconductor manufacturing and advanced packaging
- Large capacity batteries for electric vehicles
- Critical minerals and materials
- Pharmaceuticals and active pharmaceutical ingredients

After identifying vulnerable categories, governments must develop a set of critical risks to monitor these products and services. For example, critical risks impacting semiconductor manufacturing include:

- Fragile supply chains
- Malicious supply chain disruptions
- Obsolete semiconductors and related challenges to profitability

- Customer concentration and geopolitical factors
- Erosion of the U.S. microelectronics ecosystem
- Skilled worker shortages
- Intellectual property theft
- Capturing innovation benefits
- Aligning public-private interests

For governments, information sharing requires visibility into critical events, especially when national defense is involved. However, suppliers may hesitate to provide visibility to governments when warning about sustainment shortages for critical military systems. This inhibits the development of trusted customers and suppliers.

In addition, mergers and acquisitions may mean that prime vendors do not know who is in their supply network, leading to sudden disruptions when a component is no longer supported. In one case, a U.S. firm was acquired by a Chinese company, which meant that the acquired U.S. firm could no longer sell products to the U.S. government.

Another lesson learned was the importance of mapping supply chain networks to build effective supplier relationships. Machine-generated supply network maps may be inaccurate without validation. For this reason, network mapping needs organic verification based on source-level data.

Data is essential to reducing risks associated with supply chain disruption. However, data relevant to supply chains does not reside in most government systems. Commercial partners will need to be heavily involved in collecting key information.

ACTION STEPS

- Governments need to determine the areas of highest vulnerability to supply chain risks, and map their supply chain networks to recognize and build key supplier relationships that can address those risks.

Apply design thinking to develop key supply chain components
Design thinking can help governments build supply chain resiliency by developing statements of work, specifications, and sourcing networks with resiliency in mind. Effective networks must be designed at the outset of a program.

As governments build supply chain immunity in the face of shocks, they need to establish inventory stockpile requirements. Stockpiles apply not only to pandemic-related goods, but also to inventories of critical commodities such as energy, pharmaceuticals, semiconductors, aerospace components, and other national security products. Many government agencies can manage one-time disasters, but struggle with broader crises that shock supply chains daily.

Several government experts support the notion that "you will never stockpile your way out of disruption issues." To create agile domestic production capabilities at a cost-efficient price will require the further development of advanced manufacturing capabilities. However, this could run counter to national mandates, such as U.S. procurement practices that minimize cost at the expense of quality.

Stakeholder education will also be an important factor in network design. Typically, government program managers focus on cost, assessment, and scheduling. Adding supply chain resilience to these criteria would require a major shift in sourcing strategy.

This may include establishing pre-award intelligence requirements that require vendors to make business continuity plans transparent and provide location details about where materials are sourced. This change has been described as "democratization of data"—anyone working on a program can see the data and understand where disruptions may occur. To build supply chain immunity and resiliency, governments need to implement robust shared technology platforms for supply chain visibility and planning. These platforms need to include AI tools, data analytics, intelligent workflows, and supply chain mapping information to inform decision making and resource deployment.

Supply chain visibility also enables decision makers to pivot from a reactive to a predictive stance and mitigate problems before they occur. Real-time analytics and predictive modeling can support future-state planning. To develop this capacity, governments need to define a problem set and then identify the data needed to address that challenge. Supply chain visibility should occur in real time and provide transparency into the status of critical components and materials. To make sure users have total supply chain visibility, the private sector will also need to collect and share relevant data.

ACTION STEPS

- To design effective networks, governments need to establish inventory stockpile requirements, educate stakeholders to drive change, and develop technology for supply chain visibility and planning.

Sustain supply chains through risk mitigation and private sector partnerships

After establishing a visibility network and data collection protocols, a government-led supply chain shared service strategy can shift to a "sustain" mode. This includes the development of predictive models, mitigation strategies, and partnerships with private-sector organizations to innovate and expand capabilities.

Wargaming is a useful risk mitigation tool. These exercises bring together stakeholders from different functions to explore various scenarios and examine how future shocks to supply chains could impact government assets, leading to improved procurement approaches and local sourcing alternatives.

Supply chain wargaming also supports stockpile management. Participants discussed that the evolving concept of a "virtual stockpile," which enables distributors and manufacturers to hold materials within their own operations, but also provides data visibility to make these materials rapidly available to governments in a crisis.

With the growing sophistication of predictive analytical tools, governments can build on insights gained from wargaming to develop more accurate "what if" scenarios and contingency plans. Technologies such as AI and digital twins—the Port of Rotterdam uses digital twinning to visualize and make decisions quickly and effectively[4]—could also be used to find out where supply chains can break down under stress conditions.

To sustain supply chains, investments are required in resilience capabilities. However, many agencies lack the financial resources and authority to make these investments. Contract officers perennially weigh cost, schedule, and performance, often leading to trade-offs between operations and longer-term sustainment capability. Indeed, government procurement often drives other purposes and objectives, resulting in multiple goals and measures of success. Improving the resilience of government critical supply chains should be considered as a key requirement in procurement decisions, alongside product cost, life cycle costs, and environmental impacts.

Procurement also has a responsibility to act as an organized entity on the demand side. Clear demand signals create economic incentives to invest in strategic industries. These signals also increase the willingness to share data and share the development of more comprehensive business continuity plans.

Designating vulnerable industries as essential to a national economy may lead to additional challenges, such as steering investment into critical areas. This requires recognition of structural difficulties within domestic supply chains to meet economic and security objectives. If at-risk essential sectors cannot be sourced without higher costs, then governments need to invest in domestic industries that support national security, such as electric batteries, semiconductors, and pharmaceuticals.

To improve supply chain resiliency, governments must foster strong partnerships with the private sector. By sharing information and developing mutual trust, governments and businesses can help each other adjust to different situations that might arise in an unpredictable, disaster-prone world. The U.S. National Emergency Business Operations Center—part of the Federal Emergency Management Agency—has established a precedent for developing such partnerships.[5]

Measuring costs and return on investment also supports supply chain resilience. Governments often do not track these costs, nor costs related to expediting fees, emergency alternative sourcing, and overtime. And since financing often occurs through progress payments, costs are simply passed on to the government after being incurred—increasing overall costs in subsequent years.

ACTION STEPS

- To sustain a resilient supply chain, and better understand the potential impact of disruptions, governments should run war games, use predictive analytics, and improve acquisition strategies and private-sector partnerships.

Roundtable in Rotterdam, the Netherlands

For an international perspective on developing supply chain resiliency for governments, a roundtable event was held at the Port of Rotterdam in the Netherlands, where European experts added context to the action items introduced in Washington. The event was cosponsored by the American Chamber of Commerce in the Netherlands. The Port of Rotterdam—a very large government-owned entity, the largest seaport in Europe, and a key European supply chain hub—is embarking on a data-driven modernization strategy.

In the Dutch discussion, cooperation between governments and private industry emerged as essential in bringing the shared services concept to fruition. For example, the shipping industry has difficulty in obtaining and sharing data. Ports, supply chains, and transport networks each have their own API systems. In addition, governmental rules and regulations often prohibit the sharing of information between port operators and logistics providers. The ability of governments and commercial entities to exchange data on a timely basis needs to be a high priority task when building systems that support resilient supply chains.

Given the interest in recent advances in generative AI, the Rotterdam roundtable provided insights into the role that AI and other advanced technologies—such as automation and quantum computing—will play in supply chain resilience. Algorithms using these technologies have potential to optimize the operation of container-lifting cranes, direct vehicles, and help pilots bring ships safely into ports as busy as Rotterdam, which handled 467.7 million tons of goods in 2022.

However, these new technologies also represent potential risk. When discussing supply chain vulnerabilities, roundtable participants shared concerns about the security of supply chain networks. In the hands of hackers and absent strong cybersecurity protections, AI and quantum computing could disrupt logistics, customs operations, and border protection.

Roundtable participants agreed with the criticality of building security into the design of emerging technology systems to drive resiliency, rather than bolting on security only after a risk or threat arises. The Rotterdam roundtable provided insights into the benefits—and potential risks—that advanced technologies such as AI, automation, and quantum computing will have in transforming supply chain operations.

Modernize supply chains to build resilience

Building supply chain resiliency solutions starts with a strategy involving a government-led, industry-involved shared service and center of excellence. Given the central role of a shared approach to building supply chain resiliency, how can governments set up these collaborative organizations that meet their specific requirements? Though the recommendations outlined in this chapter were developed within a U.S. government context, this framework could also be applied to other democratic governments with similar agency structures.

In the U.S., a shared service for supply chain resilience could include multiple agencies that share a common objective. The European Union already has a similar framework that shares data and information among countries.[6] A shared service could span several domestic agencies with direct insights into various types of civilian and national security supply chain disruptions. These could include the Departments of Homeland Security, Commerce, Health and Human Services, Energy, Transportation, State, and Defense, as well as the Intelligence Community. Other nations may choose to house a shared services capability in ministries or bureaus with similar responsibilities.

ACTION STEPS

- Shared service capability needs to exist as a core responsibility, and the government should own it, lead it, and drive cross-border collaboration with other countries.
- Establish agency mission-support leadership roles for supply chain management that address cross-departmental and interagency component tasks.

LOOKING FORWARD

Assembling the multiple components of a supply chain resiliency solution will need more than government participation. The private sector will also need to be involved when developing this capability. For this reason, private-sector advisors to agencies should include business leaders and subject matter experts from different nodes in the supply chain. These experts could come from equipment manufacturers, distributors, logistics providers, hospitals, retail pharmacy chains, and drug manufacturers.

Governments are responsible to broad constituencies for building supply chain immunity, and a shared services center of excellence provides a practical structure to manage this responsibility. Such a strategy would integrate the expertise of government agencies with private-sector business acumen. It also provides the flexibility to anticipate and respond to continuously changing supply chain disruptions.

Endnotes

1 The 2022 CEO Study. *Own your impact: Pathways to transformational sustainability.* IBM Institute for Business Value. May 2022, https://ibm.co/c-suite-study-ceo.

2 Handfield, Robert, and Daniel J. Finkenstadt, *Supply Chain Immunity: Overcoming our Nation's Sourcing Sickness in a Post-COVID World*. 2022. Springer, https://link.springer.com/book/10.1007/978-3-031-19344-6.

3 "Building resilient supply chains, revitalizing American manufacturing, and fostering broad-based growth." A report by The White House. June 2021, https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

4 Boyles, Ryan. "How the Port of Rotterdam is using IBM digital twin technology to transform itself from the biggest to the smartest." IBM blog. August 29, 2019, https://www.ibm.com/blogs/ internet-of-things/iot-digital-twin-rotterdam/.

5 "National Business Emergency Operations Center Fact Sheet." Federal Emergency Management Agency. May 28, 2019, https://www.fema.gov/sites/default/files/2020-03/nbeoc-fact-sheet _ 2019.pdf.

6 "Data Act: Commission proposes measures for a fair and innovative data economy." European Commission press release. February 23, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip _ 22 _ 1113.