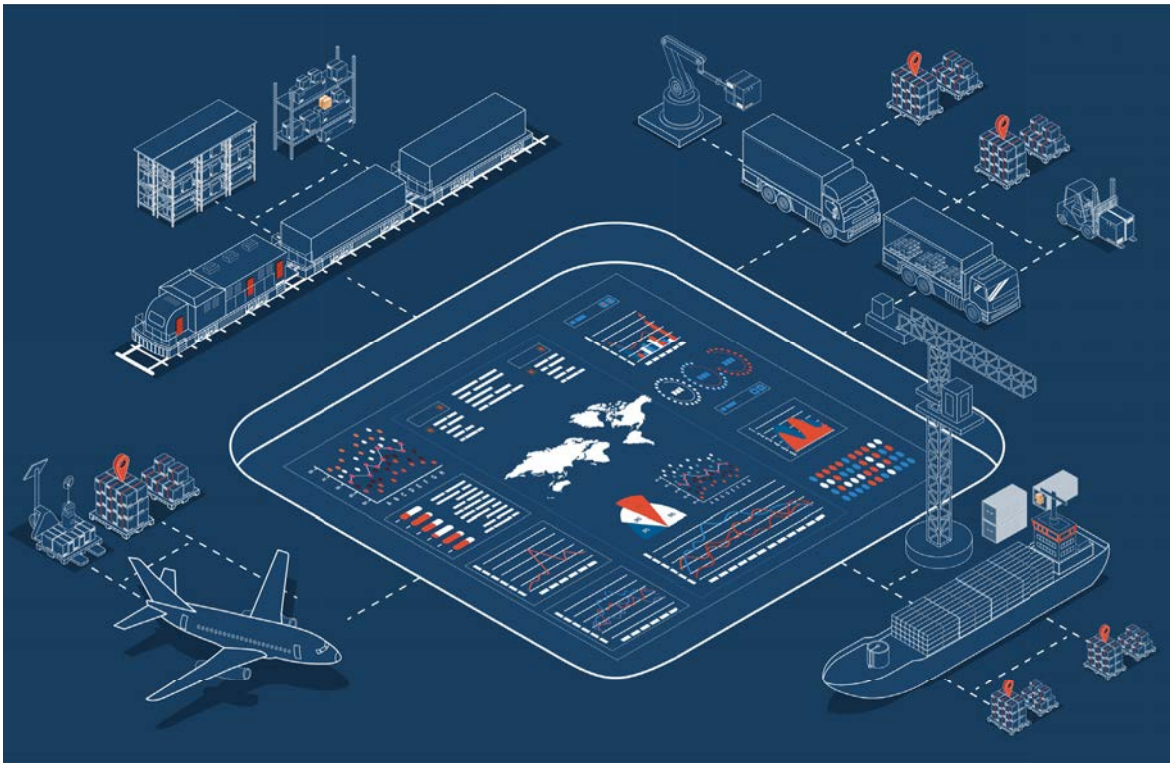
RAND

Research Report

REBECCA LUCAS, THOMAS EKSTRÖM, PAOLA FUSARO, ELIZABETH HASTINGS ROER, LUCIA RETTER

Toward Defense Supply Chain Disruption Management

A Research Agenda for Defense Supply Chain Resilience



For more information on this publication, visit **www.rand.org/t/RRA2504-1**.

Published by the RAND Corporation, Santa Monica, Calif.

Cover: Sarawut Burarak/Getty Images.

About This Report

This report represents the primary output of a study co-led by RAND, a nonpartisan, not-for-profit research organization, and the Swedish Defence Research Agency (Totalförsvarets forskningsinstitut; FOI), an assignment-based authority under the Swedish Ministry of Defence.

This project aimed to outline a research agenda to understand how defense supply chains can better withstand unanticipated and highly impactful disruptions whose probability and impact cannot be readily calculated or quantified. Specifically, the project team set out to identify the current state of the research on supply chain risk management, supply chain disruption management, and supply chain resilience, both within the defense sector and across the broader commercial landscape. The project team also explored the unique characteristics of defense sector supply chains and the ways in which practices from other sectors might or might not be applicable. Finally, as part of this research project, the team also sought to identify knowledge gaps or broader questions that might not appear in the literature. These knowledge gaps were then used to generate a research agenda. This report should be of interest to public and private sector practitioners because of its comprehensive perspective on defense supply chains.

RAND Center for Global Risk and Security

This work was undertaken by the RAND Center for Global Risk and Security, part of International Programs at RAND. The center explores systemic risks to global security, drawing on researchers' expertise in multiple disciplines to complement and expand RAND research in such fields as security, economics, health, and technology. A board of distinguished business leaders, philanthropists, and former policymakers advises and supports center activities, which are increasingly focused on global security trends and the effects of disruptive technologies on risk and security. For more information, visit www.rand.org/international/cgrs.html or contact the director (contact information is provided on the webpage).

The Swedish Defence Research Agency

FOI is a government agency under the Swedish Ministry of Defence that is primarily focused on assignment-based activities. Its largest clients are the Swedish Armed Forces, the Swedish Defence Materiel Administration, the Swedish Government Offices, and the Swedish Civil Contingencies Agency; however, it also has many assignments from other government authorities, municipalities, and companies within the defense and security fields.

Funding

Funding for this research was provided by the generous contributions of the RAND Center for Global Risk and Security Advisory Board and support from FOI.

Acknowledgments

The project team would like to thank the RAND Center for Global Risk and Security Advisory Board, King Mallory, and Robin Meili for their generous support in making this project possible. We would also like to thank Krister Pallin at FOI for being so generous with Thomas Ekström's time on the project, which was also a key enabler for this project. Finally, we would like to thank Julia Muravska, former research leader in Defense and Security at RAND Europe, for helping to put together the initial proposal and provide guidance in the first six months of the project. It is thanks to her input and expertise that this project and this report ultimately came into being.

We are grateful to the numerous experts whose contributions were critical to the writing of this report and validating the associated research agenda. In particular, we acknowledge the generous inputs of our interviewees and the participants in a workshop conducted in January 2023. While they will remain anonymous, their affiliations are listed in Appendix B.

We would also like to thank our quality assurance reviewers for their thoughtful and insightful comments: Erik Silfversten, research leader in Defense and Security at RAND Europe; James Black, research leader in Defense and Security at RAND Europe; Bradley Martin, director of the RAND National Security Supply Chain Institute and senior policy researcher; and Peter Watkins, CBE, RAND Europe associate and former director general for Strategy and International, United Kingdom Ministry of Defence.

Summary

Scholars and Practitioners Agree That Risks to Defense Supply Chains Need Active Management But Do Not Agree on How to Enhance Supply Chains' Resilience Vis-à-Vis Disruptions

In the past several years, global headlines have repeatedly cited significant, severe disruptions to global supply chains that are of a new and arguably unprecedented scale (Aboagye et al., 2022; Jones, 2022; Leslie, 2022; Maidment, 2010; Shih, 2020). Although the likelihood of these "one-in-100-year events" has been perceived to be quite low, the rate of their occurrence has seemed to increase in recent years. Causes of supply chain disruptions span such events as volcanic eruptions, the coronavirus pandemic, ransomware attacks, U.S. sanctions on China, and the cascading impacts of the Russian invasion of Ukraine, and the increasing number of these events has demonstrated that disruptions can propagate quickly through supply chains, crippling companies' operations and ability to deliver goods and services. An interest in addressing the threat that these severe, unanticipated disruptions (sometimes referred to as *black swans*[1] or *unknown unknowns*[2]) can pose to supply chains has consequently become increasingly prominent.

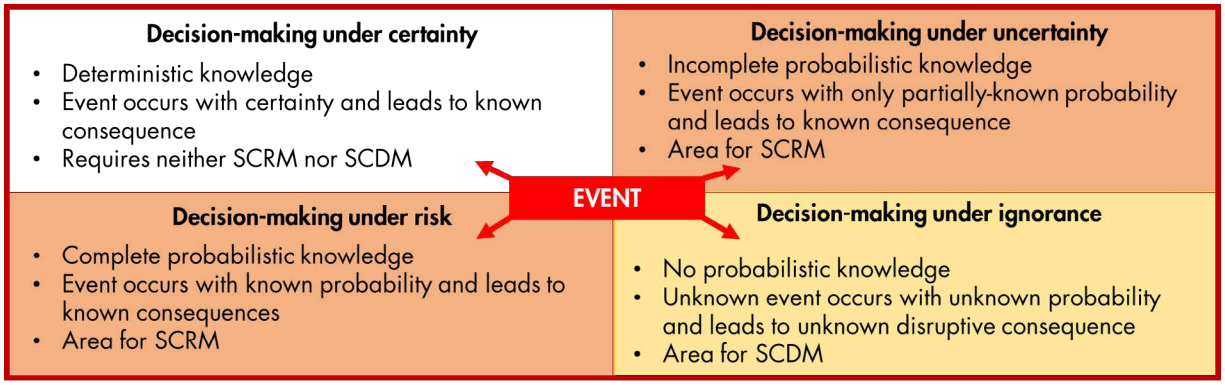
On top of more traditional supply chain risk management (SCRM) approaches, researchers and practitioners have consequently sought to mitigate supply chain disruptions by enhancing supply chain resilience (SCRES). Unlike SCRM, however, *SCRES* is defined as the ability of a supply chain to prepare for, respond to, and recover from disruption, either by resuming its previous state or moving to a more optimal configuration; it is therefore a property of supply chains rather than a management approach. Furthermore, SCRM approaches assume that potentially disruptive events are predictable, requiring identification and quantification of disruption risk. This assumption leaves a host of unforeseen and unquantifiable risks for which SCRES is not being actively addressed. Therefore, we draw a distinction between SCRM, which addresses events whose probability and impact can be calculated, and supply chain disruption management (SCDM), or efforts to mitigate these unknown unknowns through enhancing SCRES. Despite increasing interest in SCRES, SCDM remains an

[1] Popularized by Nicholas Nassim Taleb, *black swan events* are categorized as rare events whose likelihood is difficult or impossible to assess (Taleb, 2017). A black swan event is often characterized by three main attributes: The event is an outlier that sits outside of regular expectations; its consequences have extreme impacts; and it is only predictable in retrospect (Olivares-Aguila and Vital-Soto, 2021).

[2] The concept of *unknown unknowns* was popularized by Donald Rumsfeld in his famous 2002 remarks (U.S. Department of Defense, 2002). This project related Rumsfeld's three categories to the Johari window to establish four quadrants of decisionmaking: decisionmaking under certainty (known knowns), decisionmaking under uncertainty and risk (unknown knowns and known unknowns), and decisionmaking under ignorance (unknown unknowns) (Luft and Ingham, 1955).

understudied area, often conflated with traditional, quantifiable SCRM. Figure S.1 lays out areas in which SCDM is necessary, as opposed to SCRM.[3]

Figure S.1. Quadrants for SCRM Versus SCDM



SOURCE: FOI research based on Hansson (2005).

In addition, SCRES research has focused on the commercial sector; however, defense supply chains also face unique challenges given their different structures, dynamics, and characteristics: For example, they have a relatively high level of government interference given the monopsonic nature of the market. Additionally, the consequences of supply chain disruptions in the commercial sector are typically calculated in monetary terms; however, for defense supply chains, such a reduction could undermine success of operations and ultimately national security. This then raises a question of whether existing SCRM, SCDM, and SCRES research is suitable for defense supply chains and where or how it may need to be complemented by further research that is better tailored to a defense context.

RAND and FOI Propose a Research Agenda to Help Enhance Understanding of Defense Supply Chain Resilience and Disruption Management

Given the significant gaps in understanding of how defense supply chains can better resist and recover from disruptions and what disruption management might require, the RAND Center for Global Risk and Security sponsored this study, which was conducted jointly by researchers from RAND and FOI. The purpose of the study was to identify gaps in supply chain management (SCM) research from a defense perspective and to propose a research agenda to help build understanding of how defense supply chains can better withstand severe, unanticipated disruptions.

The study shows that more research is required to identify good strategies for SCDM for defense, as well as how supply chain specialists and defense and security policymakers might implement these strategies across both the private sector and government. This report therefore sets out a research agenda to help fill existing gaps in understanding of how defense supply chains can better resist and

[3] The four quadrants presented here are based on a model devised by the Swedish Defence Research Agency (Totalförsvarets forskningsinstitut; FOI) using research by Hansson and others and will be explained in detail later in the report.

recover from disruption. The main gaps in understanding as identified by this research agenda also represent some of the key enablers for effective defense SCDM. These research areas are as follows:

- Improve understanding of supply chain disruption, including the composition of defense supply chains and their associated stakeholders and actors.
- Determine which commercial sector approaches to SCDM can be adapted for or adopted by defense.
- Recognize and tackle challenges for SCDM that stem from the multisectoral nature of defense supply chains.
- Clarify and distinguish between SCRM and SCDM to understand the benefits and challenges of each approach.
- Define what resources are needed to enable implementation of defense SCDM.

Within each of these research areas, the study team identified several potential questions, which are detailed in the sections that follow.

Improved Understanding of Supply Chain Disruption in Defense Supply Chains

The research repeatedly showed that defense supply chains have unique needs and challenges depending on the sectors that they cross, the stakeholders they involve, and the nature of their end products. Broad, theoretical questions are important for understanding of the scope of disruption management. A more detailed understanding of the defense supply network, and individual defense supply chains, requires investigation to understand the most effective approach to SCDM. Specific research questions in this area might include the following:

- What risks and vulnerabilities are specific to defense supply chains or exist across multiple defense supply chains?
- How are SCRES requirements affected by the different ways that governments evaluate the costs of defense supply chain disruptions? How might these implications be different during a time of geopolitical conflict, such as war?
- What tools, techniques, and methodologies can governments and companies use to better understand and monitor their defense supply chains, including the multiple tiers of subcontractors?
- What replicable examples of good practice have been used in defense supply chains that might be applicable to other defense or commercial supply chains?
- How can governments ensure that private sector suppliers in defense supply chains have the key tools needed to conduct SCDM and enhance SCRES?
- To better understand SCRES, how is *recovery* defined? Can time to recovery be measured?

Applicability of Commercial Sector Approaches to Supply Chain Disruption Management in Defense Supply Chains

As discussed previously, the research showed many differences between defense and commercial supply chains in terms of their structure, their nature, and the implications of disruption. A key gap identified is the ways in which disruption management approaches and strategies generated for commercial supply chains might apply to the unique characteristics of the defense sector. Specific research questions in this area include the following:

- How can commercial supply chain disruptions impact their defense sector counterparts?
- What is the appropriate role of government in SCDM for the commercially owned segments of defense supply chains, given the unique requirements of defense supply chains?
- How do the differences between defense and commercial supply chains impact the relevance of commercial sector approaches? Are any commercial sector SCDM approaches appropriate or beneficial given the unique requirements of defense?

Challenges for Supply Chain Disruption Management from the Multisectoral Nature of Defense Supply Chains

Supply chains in both the commercial and defense sectors often have global reach and dependencies on diverse areas of national infrastructure (e.g., energy, transportation, communications, or banking networks). Therefore, the research suggests that effective defense SCDM may involve industry-wide, nationwide, or even multinational approaches. Given the national security implications of disrupting defense supply chains, this could be an area for government intervention; however, there is no consensus on the appropriate nature and extent of such intervention. Specific research questions in this area might include the following:

- What are some of the current enablers and barriers to cooperation between the private and public sectors in terms of defense SCDM?
- How can governments better collaborate with partners and allies to enhance the resilience of international defense supply chains or limit defense supply chains' exposure to potential adversaries (e.g., offshoring/ally-shoring)? What are the limits of such collaboration?
- To what extent might SCDM approaches in defense connect to broader discussions of societal resilience?

Distinguishing Between Risk Management and Disruption Management Approaches in Defense

The research clearly distinguishes between SCRM, which mitigates risks that are at least partially understood, and SCDM, which aims to enhance overall resilience to respond to and recover from unanticipated disruptions. Further research is required into where SCRM and SCDM approaches might be appropriate, as well as how they might complement each other in defense SCM. Specific research questions in this area might include the following:

- What further distinctions can or should be drawn between SCRM and SCDM to better enable defense practitioners across industry and government to address both areas?
- In a defense-specific context, what are the respective strengths and weaknesses of SCRM and SCDM?
- Can SCRM and SCDM approaches complement one another in enhancing defense SCRES? If so, how?

Resourcing and Prioritizing Defense Supply Chain Disruption Management

The research confirms that a drive for lean or efficient approaches to SCM may have detrimental effects for SCRES. Despite the recognition of the importance of resilient supply chains, the financial constraints that drive these lean and efficient approaches are unlikely to abate. To the extent that supply chain leanness degrades SCRES, supply chain professionals may therefore need to be able to demonstrate the need for SCRES and the value for money of SCDM. Specific research questions in this area might include the following:

- What are some of the current or anticipated barriers and enablers for resourcing and implementing SCDM approaches in defense across different actors (e.g., government, private sector)?
- What are the key resources needed by practitioners in both government and the private sector to design and implement SCDM strategies in defense?
- What kinds of key performance indicators can be used to measure the performance of SCDM approaches in defense? How can the value for money of different approaches be demonstrated or understood in defense?

It is the project team's hope and ambition that this research agenda will help support and encourage further inquiry in this key area for defense supply chains by academics, practitioners, government, or private sector stakeholders, including defense industry, national ministries of defense and armed forces, and the traditional defense and security policymaking community.

Contents

Figures and Tables

Figures

Tables

Chapter 1

Introduction

1.1. Background

Defense supply chains are integrated into globalized supply chains and thus are vulnerable to disruptions stemming from war, terrorism, pandemics, and natural disasters. Supply chain disruptions are not new but have been brought to public attention most visibly by the large-scale effects on supply chains resulting from the volcanic eruptions in Iceland (2010), the coronavirus disease 2019 (COVID-19) pandemic (2020 onwards), and, most recently, the cascading impacts of the war in Ukraine (February 2022 and ongoing); these disruptions have often been exacerbated by contemporaneous and unpredicted spikes in demand. These and other disruptive events have clearly demonstrated that disruptions can propagate through supply chains more quickly than decisionmakers can effectively respond to them and can cripple companies' operations and deliveries of products (Abogaye et al., 2022; Jones, 2022; Anuat, Van Bossuyt, and Pollman, 2022; Hitchens, 2020; Janes Intelligence Briefings, 2020; CNBC, 2019; Ferry and Poindexter, 2016). This disruption can be detrimental and even catastrophic to economic activity and can have highly damaging impacts on defense operations and the ability of armed forces to carry out their tasks.

Researchers and practitioners have anticipated and sought to mitigate supply chain disruptions through supply chain resilience (SCRES) as a complement to supply chain risk management (SCRM). In this context, *SCRES* is defined as the ability of a supply chain to prepare for, respond to, and recover from disruption, either by returning to its original state or by moving to a new, more desirable state. However, SCRM approaches assume that potentially disruptive events are predictable, requiring identification and quantification of disruption risk. In addition, SCRES research has focused on the private sector, in which a temporary reduction in capabilities may be commercially acceptable and companies must weigh the costs of proactive and reactive strategies against the potential costs of doing nothing. For armed forces, such a reduction could undermine the success of operations and, ultimately, national security. This raises the question of how suitable SCRES research is for defense supply chains and where or how it may need to be complemented by further research that is better tailored to addressing supply chain disruptions in a defense context.

The diversity and lack of predictability associated with the recent supply chain disruptions have caused some experts to argue that SCRM is no longer sufficient and that more resilience-based thinking is needed instead.[4] Therefore, this project team proposes, in line with a few other academics, to use the term *supply chain disruption management* (SCDM) to describe how managers should think about addressing disruptive events (Dolgui and Ivanov, 2021; Altay and Pal, 2022). Further sections of this

[4] Katsaliaki, Galetsi, and Kumar, 2021; Ali, Mahfouz, and Arisha, 2017; Nakano and Lau, 2020; participant in workshop conducted by RAND and Swedish Defence Research Agency (Totalförsvarets forskningsinstitut; FOI), January 11, 2023.

report will distinguish between SCRM and SCDM in more detail and expand upon the need for SCDM, particularly in defense supply chains. Additionally, we hope that this report will help bridge an existing gap between supply chain management (SCM) researchers and the traditional defense and security policy community, given the particular importance of SCDM that the project team perceives for defense supply chains.

1.2. Project Objectives

This report is the final output of a project conducted by researchers from RAND and FOI. Funding for this research was provided by the generous contributions of the RAND Center for Global Risk and Security Advisory Board and support from FOI. This project aimed to investigate how defense supply chains can better withstand unanticipated and highly impactful disruptions. Specifically, the project team set out to identify the current state of the research on SCRM, SCDM, and SCRES, both within the defense sector and across the broader commercial landscape. As part of this research project, the team also sought to identify knowledge gaps or broader questions that might not appear in the literature. This work draws on an extensive review of the literature, as well as expert interviews and a validation workshop, all of which are described in more detail in Appendix B. Overall, this report aims to improve the understanding of defense supply chains to support further research on supply chain disruptions and encourage a better understanding of how SCRES can be improved through SCDM.

1.3. Scope and Definitions

This project was specifically concerned with supply chains in the defense sector, the definition for which is provided in the box below. This definition is intended to distinguish defense sector supply chains from commercial supply chains, which the project team has used in this paper to refer to sectors outside of defense and outside of other government procurement.[5]

Definition of Defense Supply Chains

For the purposes of this project, *defense supply chains* refers to those supply chains that are **intended to provide military-specific supplies to ministries of defense and the armed forces** of various countries.

SOURCE: RAND and FOI research.

In looking at defense supply chains, the project team necessarily had to make some trade-offs to make the research project manageable within its parameters:

[5] While the project team recognizes that the private sector and commercial companies are intimately involved in defense supply chains, the team believed this was the best way to delineate the defense sector as opposed to other areas that, for example, feed into industrial or consumer markets.

- This research project focused primarily on the **broader networks through which goods are assembled and manufactured** before coming under the control of the armed forces; it therefore is not specifically concerned with the logistics of last-mile or battlefield resupply.[6]
- This research **considered defense supply chains as a general category**, rather than examining the unique needs of any individual supply chain.
- This research is primarily based on the insights of **those in academia studying disruption management in defense supply chains, as well as practitioners in government**. The research agenda therefore more closely reflects their priorities and insights. However, while they were not the primary focus of this research, private sector practitioners, as well as other public sector authorities and practitioners, should also find insights of interest in this work and the proposed research agenda.

North Atlantic Treaty Organization Definition of Logistics

The North Atlantic Treaty Organization (NATO) defines *logistics* as "The science of planning and carrying out the movement and maintenance of forces. In its most comprehensive sense, the aspects of military operations which deal with: design and development, acquisition, storage, transport, distribution, maintenance, evacuation, and disposal of materiel; transport of personnel; acquisition or construction, maintenance, operation, and disposition of facilities; acquisition or furnishing of services; and medical and health service support."

SOURCE: NATO (2012).

During its research, the project team found a great deal of literature looking at SCM across a variety of sectors, such as health care, consumer products, and electronics. This report defines *supply chains* as complex networks, which include interconnected firms, facilities (e.g., for manufacturing, warehousing, or distribution), and customers or end users, as well as products and processes (Bier, Lange, and Glock, 2020; Maharjan and Kato, 2022). A supply chain is constituted by the entities that are engaged in the upstream and downstream flows of goods, services, information, and capital (Mentzer et al., 2001), in a network of nodes, including suppliers, production centers, warehouses, distribution centers, and customers (Maharjan and Kato, 2022), from raw material extraction to end-user consumption (Handfield and Nichols, 1999). It also consists of all the activities that these entities, such as manufacturers and distributors, perform to create value, including purchasing, manufacturing, and distribution (Chen and Paulraj, 2004). The sprawl and complexity of supply chains is often a key driver of the vulnerability of these chains to anticipated and unanticipated disruption. Avoiding these disruptions requires that supply chains have the property of resilience, described in the box below.

[6] The United Kingdom Ministry of Defence (UK MOD) defines *last-mile resupply* as "the delivery of combat supplies from the forward-most location (such as a physical base or a logistics/infantry vehicle) to personnel engaged in combat operations" (UK MOD, 2017).

Definition of Supply Chain Resilience

SCRES is the ability of a supply chain to prepare for a disruption, respond to it, and recover from it and return to normal operations, or move to a more desirable state, quickly, efficiently, and effectively.

SOURCE: RAND and FOI research based on Ali, Mahfouz, and Arisha (2017); Maharjan and Kato (2022); Melnyk et al. (2010); Ponomarov and Holcomb (2009); Ribeiro and Barbosa-Povoa (2018); and Sheffi and Rice (2005).

In the box below, we present the definitions of SCDM and SCRM as devised for use in this project. More detailed discussions of how and why the project team came to these definitions and how SCRM and SCDM differ follow in subsequent chapters.

Definition of Supply Chain Disruption Management

SCDM is the process of process of designing and implementing proactive, concurrent, and reactive strategies that enhance the ability of supply chains to prepare for a disruption, respond to it, and recover from it and return to normal operations, or move to a more desirable state, quickly, efficiently and effectively.

SOURCE: RAND and FOI research based on Ali, Mahfouz, and Arisha (2017); Maharjan and Kato (2022); Melnyk et al. (2010); Ponomarov and Holcomb (2009); Ribeiro and Barbosa-Povoa (2018); and Sheffi and Rice (2005).

This definition was created in part to clearly distinguish SCDM from its more common counterpart, SCRM. The definition that this report uses for SCRM is presented in the box below.

Definition of Supply Chain Risk Management

SCRM is the process of identifying, assessing, quantifying, and monitoring potential risks that might disrupt the supply chain, as well as potential measures to prevent or mitigate their impact.

SOURCE: RAND and FOI research based on Aqlan and Lam (2015); Vilko, Ritala, and Hallikas (2019); Ferry and Poindexter (2018); Davis and Sullivan (2017).

1.4. Caveats

This research project is subject to a few caveats:

- Despite the existence of a large body of literature on SCM more broadly, there is **limited literature available covering SCM in the defense sector**, particularly SCDM.
- Although this report has tried to define key terms as they are used in the context of this report, **the project team identified multiple contradictory uses of terminology**, including *supply chain*, *disruption*, *risk*, and *resilience*. Therefore, some terms are used in a particular context here that may not match their use in other contexts or areas of the literature.
- Because this was a scoping study, **timelines and research funding necessarily constrained the number of possible interviewees, as well as the amount of literature** that the project team was able to review. There may be sources that were neglected, despite our best efforts.

Therefore, the interviews cited here do not provide a comprehensive overview or systematic review of the field but instead represent what the project team was able to gather within the constraints of this project. Further research is therefore needed to build a more comprehensive view.

- SCM is a dynamic field with ever-shifting risks and sources of disruption. Technology, too, plays a key role in SCM practices. **Although this report tries to be as comprehensive as possible, it is likely that there are aspects that it was not able to address.**

1.5. Report Outline

This report proceeds as follows:

- **Chapter 2** provides a brief introduction to SCDM across a range of sectors, based on existing literature.
- **Chapter 3** explains the unique features of defense supply chains and discusses the current state of SCDM in the defense sector.
- **Chapter 4** expands on barriers to SCDM specifically in defense supply chains.
- **Chapter 5** outlines overarching conclusions before presenting the research agenda to help support future researchers in addressing some of the most pressing gaps.

This report also includes two appendixes:

- **Appendix A** is a stand-alone version of the research agenda (designed for independent presentation).
- **Appendix B** presents our study methodology.

Chapter 2

Conceptualizing Supply Chain Disruption Management

This chapter first discusses the study team's understanding of the differences between risks and disruption. It then moves on to highlight general SCM practices, aiming to explain where SCDM fits into those practices and how the study team has developed its understanding of SCDM as distinct from SCRM. The chapter then zooms in on articulating the need to consider SCDM as an unavoidable part of effective SCM in the future.

2.1. Risks Versus Disruptions

In academic and gray literature, the terms *risk* and *disruption* are often used interchangeably or to describe one single phenomenon (e.g., *disruption risk*, which is discussed below). However, they refer to different, if closely related, concepts. Simply put, disruptions refer to *what* happens to supply chains, whereas risks also consider *whether* a disruption happens and the extent of its impact. For the purposes of this report, we define *disruptions* as **events that modify the normal flow of goods and materials within supply chains, irrespective of their source, their level of predictability, and the extent of their impact**. This definition is in keeping with some academic literature**,** which has defined *supply chain disruption* as "an event or situation that interacts with the supply chain and has the potential to modify the supply chain's ability to deliver to expected time and quality conditions" (Summers, 2018). In contrast, the project team has chosen to use the term *risks* to refer to the probability and impact of possible disruptions in the event that they **can be identified, monitored, and forecast, with their probability and/or impact estimated**.[7]

2.1.1. Endogenous and Exogenous Risks and Disruptions

Both **risks and disruptions can originate from either within the supply chain** (*endogenous*) **or outside of it** (*exogenous*) and cause shocks to supply chains (Summers, 2018). These shocks can impede or entirely interrupt some or all of the operations that constitute a supply chain. Of note, one of the interviewees for this study identified three mutually reinforcing and interdependent flows that are the focus of SCM: products, information, and finances.[8] These flows can be interrupted by either risks

[7] Prahasi et al. (2021), Olivares-Aguila and Vital-Soto (2021), and Duong and Chong (2019) all discuss the fact that disruptions cannot be quantified as one of their unique features, leading the project team to determine that a clear distinction was necessary.

[8] Interview L, subject-matter expert, interview with the authors, November 29, 2022.

or disruptions, and the loss of one can and often does impact the others—for example, the loss of information systems can interrupt product flow, with a knock-on impact on finance flows.[9]

Internal (endogenous) shocks are often referred to as *operational risks*: risks that originate from within the supply chains, such as quality or safety recalls, equipment malfunction, or fluctuations in demand (Ferry and Poindexter, 2018). Endogenous events are often generated either by a *nodal failure* that is at production, storage, or user locations (e.g., quality issues located at a certain factory) or by a *chain failure* that is from the flow of goods, services, and information connecting the nodes (e.g., competitors or suppliers that are integrated with the same global supply chain but developing different strategies or working practices; Summers, 2018).

External (exogenous) shocks can come from an even broader variety of sources and are the source of most supply chain disruptions. Frequent examples include severe weather events, such as tropical storms or flooding; lack of transport availability (e.g., from grounding of flights or lack of access to trains); lack of labor availability (e.g., from disputes or strikes); deliberate attack (e.g., terrorist attacks); and closed borders (e.g., due to a pandemic, quarantine, or sanctions). Some of these shocks can be anticipated and their effects mitigated: For example, flood defenses can help reduce the risk of road closures in the wake of storms. However, others fall under the category of *unknown unknowns*[10] or *black swan events*.[11] Regardless of the precise terminology used, such events are characterized by the inability to calculate their probability or impact.[12]

2.1.2. Ripple Effects of Risks and Disruptions

Ripple effects **occur when the impacts of an event cascade throughout the supply chain instead of remaining confined to a single node or portion of the network** (Anuat, Bossuyt, and Pollman, 2022). Their propagation across the supply chain can further amplify the initial impact beyond what might reasonably be anticipated (Xiong et al., 2020). Both risks and disruptions can produce cascading effects that are unanticipated or that exacerbate the impact of a foreseen event. Ripple effects mean that even events that begin as an understood risk can interact and cascade, rapidly becoming unforeseen and unanticipated disruptions.

---

[9] Interview L.

[10] The concept of *unknown unknowns* was popularized by U.S. Secretary of Defense Donald Rumsfeld in his famous 2002 remarks: "Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones" (U.S. Department of Defense [DoD], 2002).

[11] Popularized by Nicholas Nassim Taleb, *black swan events* are categorized as rare events whose likelihood is difficult or impossible to assess (Taleb, 2017). A black swan event is often characterized by three main attributes: The event is an outlier that sits outside of regular expectations; its consequences have extreme impacts; and it is only predictable in retrospect (Olivares-Aguila and Vital-Soto, 2021).

[12] Numerous debates arose throughout the course of this study as to how to categorize such events (e.g., was COVID-19 a black swan event?) and whether such predictions have been prevented by human bias or inherent unknowability. One can also get lost in a veritable multicolored zoo of jellyfish, elephants, and rhinoceros used to categorize such events. Although such debates are of academic interest, for the purposes of this report, the project team determined that the critical characteristic was the lack of information that all of these events have in common and focused on events that are not predicted or unfold significantly differently to whatever manner was predicted, regardless of the reason for that.

Modern supply chains' expansive scale, geographical footprint, and node interconnectivity and interdependency have implications for the occurrence and nature of this phenomenon (Mian et al., 2020). Some authors note that ripple effects give rise to *ecosystem accidents*, in which systems or nodes thought to be autonomous are found to be unexpectedly interdependent, leading to a quick propagation of risks or disruptions across the supply chain (Sobb and Turnbull, 2020). Furthermore, disruptions can be interconnected, meaning that they fuel one another. This is often true for economic disruptions, which usually entail additional political or social disruptions (Summers, 2018). Finally, other authors emphasize that measures to mitigate one disruption can exacerbate another (Chopra and Sodhi, 2004). One example of this is bare-bones inventories, a practice that decreases the economic impact of overforecasting demand but can also amplify the impact of a disruption on the supply chain (Chopra and Sodhi, 2004).

The impact of COVID-19 across global supply chains illustrates some mechanisms of ripple effects. Some authors have argued that the different supply chain disruptions provoked by COVID-19 were "non-linear and temporal, arising at many different places in the supply chain[s] and sometimes at different times," with triggers occurring "often peripherally beyond the latent sphere of their extended supply networks" (Narayanan and Altay, 2021) In this context, experts suggest that SCRES strategies would be useful to tackle global disruptions and their impact across diverse supply chains (Golan, Jernegan, and Linkov, 2020). More specifically, others note that proactive redundancy (e.g., inventory redundancy) and flexibility measures are the best ways to mitigate ripple effects (Dolgui, Ivanov, and Solokov, 2018). Finally, others suggest decentralizing supply chain systems through the use of new technologies to allow different nodes to recover at different rates and to encourage more-flexible and more-independent supply chain systems and hierarchies instead of a top-down control (Osinga, 2016).

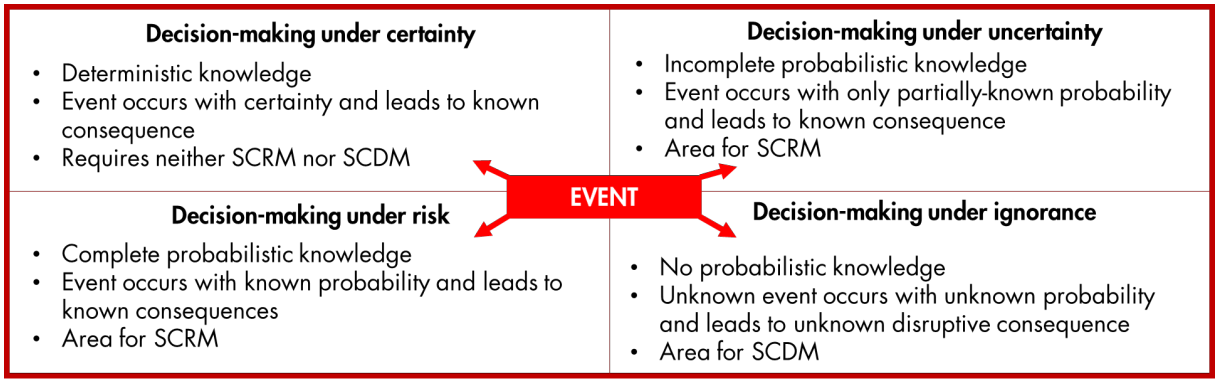
2.1.3. Decisionmaking in the Face of Risks and Disruptions

To highlight the fog and complexity under which decisionmakers operate in the face of a large-scale disruption, the project team drew on the definitions presented above, in combination with classical decision theory,[13] modern decision theory,[14] and the Johari window (Luft and Ingham, 1955), to devise its own categorization of the conditions under which decisionmaking takes place. This categorization, which underpins the team's understanding of supply chain disruptions versus supply chain risks, is presented in Figure 2.1.

[13] This theory encompasses decisionmaking under certainty (each action leads to a specific outcome), risk (each action leads to one of a set of possible specific outcomes with a known probability), or uncertainty (each action leads to one of a set of possible specific outcomes with an unknown probability) (Peck, 2006; Hansson, 2005).

[14] Modern decision theory adds *ignorance* to the set and proposes the following knowledge situations: decisionmaking under certainty (deterministic knowledge), risk (complete probabilistic knowledge), uncertainty (partial probabilistic knowledge), or ignorance (no probabilistic knowledge) (Hansson, 2005, p. 28).

Figure 2.1. The Four Quadrants of Decisionmaking



SOURCE: FOI research based on Hansson (2005).

The quadrant of "decisionmaking under certainty" requires neither SCRM nor SCDM. The quadrants of "decisionmaking under uncertainty" and "decisionmaking under risk" are both characterized by at least partial knowledge. The study team would argue that, therefore, they are addressed through the practices of SCRM. The fourth quadrant, however, "decisionmaking under ignorance," refers to threat management that must occur in the absence of any additional information. It is therefore the quadrant that requires SCRES and thus, as we argue below, SCDM.

2.2. Scope and Benefits of Supply Chain Risk Management

SCRM is often categorized as more traditional risk management that is best suited to addressing familiar, static, or predictable threats (Christopher and Peck, 2004). Traditional SCRM is the **process of identifying, assessing, quantifying, and monitoring potential risks that might disrupt the supply chain**, as well as potential measures to prevent or mitigate their impact (Aqlan and Lam, 2015; Vilko, Ritala, and Hallikas, 2019; Ferry and Poindexter, 2018; Davis and Sullivan, 2017). SCRM can involve identifying internal and external shocks that might affect supply chain operation, as well as the vulnerable points that they are most likely to impact (Ferry and Poindexter, 2016). Furthermore, it can calculate the likely impact of such shocks, either in terms of physical effects or financial costs.

Consequently, **SCRM is primarily a risk-based approach** that requires identifying the specific risks to the supply chain against potential mitigation or defensive measures (Ferry and Poindexter, 2016). It therefore tends to be more responsive and responds to specific risks that have been identified (Van Kampen, Van Fenema, and Faber, 2016). It requires looking at a specific threat or disruption and the potential responses or needs should it occur in order to limit its likelihood and mitigate its impact on the supply chain (Ryczynski and Tubis, 2021). Risk management therefore, by nature, focuses on foreseeable, predictable disruptions in which the likelihood of an event, as well as its impact, can be calculated. One of the interviewees for this study noted that even large-scale disruptions, such as those caused by pandemics, can be predicted as general trends or potential risks; perhaps the true nature and impact of individual events (such as the COVID-19 pandemic) may not be possible to prepare for, but

decisionmakers can prepare for a pandemic as a risk category.[15] Similarly, the interviewee noted that, while a specific conflict may not be possible to anticipate, more general risk categories of geopolitical tensions do tend to be captured in risk registers and considered as part of risk management.[16] SCRM is therefore a process that can be used to address all decisionmaking situations in which there is at least partial information.

Scenarios with partial information, and in which SCRM can therefore be used, are often conducive to successful outcomes. For example, if the scenario remains quantifiable, it is therefore arguably more commercially and financially justifiable to commit resources to it (Van Kampen, Van Fenema, and Faber, 2016). Furthermore, there are many established tools available for risk assessment and understanding; many of these tools have expanded their reach and ability because of advances in technology.[17] Developments in technology—such as sensors and blockchain to track the extent of supply chains, open source intelligence and data mining, and information systems and analytics that leverage artificial intelligence—are increasingly expanding the types of shocks that can be addressed with SCRM. [18]

Traditional SCRM also matches well with traditional economic approaches to SCM: As one interviewee described, "the buyer assessing their bottom line . . . is how [risk] measures are typically quantified."[19] In such calculations, the cost of a potential risk mitigation (e.g., flood defenses) is weighed against the potential cost and likelihood of the risk (e.g., a flood). A decision can then be taken on which approach maximizes profit. This therefore makes the costs and benefits of SCRM easier to weigh against the potential cost of inaction.

Examples of SCRM include implementing weather monitoring systems and emergency preparedness measures in areas that are prone to natural disasters (e.g., earthquake, flooding). In such a scenario, companies can, for example, calculate the cost of building a factory on higher ground rather than locating it in an area that has become a floodplain because of climate change, as opposed to the potential cost of losing production capability because of a flood. Other examples might include contracting with more than one trucking company or with trucking companies that employ workers from different unions, in the event of a truckers' strike. In such cases, a supply chain manager can calculate the cost of implementing a measure that might enhance resilience (e.g., an alternative provider of transport) versus the cost of temporarily losing the ability to transport a particular product.

2.3. Pursuit of Supply Chain Resilience

The rise of unanticipated or hard-to-anticipate disruptions has led to an increased interest in enhancing SCRES. The term *SCRES* is often used to describe an ability, capability, or management activity separate from SCRM, all of which are different. This project therefore uses the definition of *SCRES* **as a characteristic or property** of a supply chain that can be increased or decreased through

[15] Interview B, subject-matter expert, interview with the authors, November 18, 2022.

[16] Interview B.

[17] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[18] Interview L.

[19] Interview J, subject-matter expert, interview with the authors, December 5, 2022.

certain practices. SCRES is *risk agnostic*, referring to the ability of the supply chain to react to any threat or interruption from any source (Mian et al., 2020). Additionally, SCRES operates under the assumption that there are threats that cannot be or were not mitigated, and, thus, despite managers' best efforts, **shocks will interrupt the operation of supply chains**. Therefore, mitigating a disruption in an effort to prevent disruption is insufficient: Supply chains need to be enabled to reconfigure themselves once disrupted in order to restore functionality.[20] SCRES is therefore better suited than SCRM to cope with and respond to unpredictable events in which likelihood and/or potential cost are difficult to calculate.

While there is no consensus in the literature, some researchers suggest that there has been **a shift in SCM from traditional, reactive risk management thinking to proactive resilience-building strategies**, indicating a recognition that new approaches are needed (Nakano and Lau, 2020). These new strategies are intended to enable supply chains to anticipate, adapt to, respond to, and recover promptly from a range of risks and disruptions (Ponomarov and Holcomb, 2009). One interviewee noted that resilient supply chains are those that are flexible, in that they can sustain shocks but can also adapt quickly.[21]

Many advocate for SCRM's role in increasing resilience. This can be done, for example, through the creation of buffers to cushion supply chains from interruption, such as stockpiles or excess production capacity, or creating redundancy in production or transport locations to mitigate against predictable weather events, such as flooding or tropical storms.[22] New requirements for cybersecurity are another example of SCRM that seeks to respond to known risks: Cybersecurity risks are known to exist, even if the specific attacker may not be known. The expanding ability of technology to map supply chains, understand the likelihood of potential interruptions due to things like weather events, and forecast their impact has expanded the space in which SCRM can be used to mitigate against the potential sources of interruptions to supply chains. Certainly, SCRM can help to enhance SCRES in certain areas by increasing the number of events that are understood and quantified, so as to present a risk rather than a disruption. Indeed, **many SCRM measures enhance the ability of supply chains to continue with little or no interruption in response to a set of known risks**. In addition, the number of risks that can be known, as mentioned previously, is constantly increasing, in no small part because of technological development.

However, this ignores a key characteristic of resilience, specifically the acknowledgment that interruptions cannot be avoided entirely with certainty.[23] Therefore, based on the definitions used by this project team, **the risk-based SCRM approach necessarily cannot fully enhance SCRES.**[24] Recent events impacting supply chains, such as volcanic eruptions, COVID-19, the Russian war in Ukraine, and trade wars between the United States and China, have caused supply chain crises that were unforeseen or that varied significantly from the predicted impact of more generically articulated risks.[25]

[20] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[21] Interview B.

[22] Interview I, subject-matter expert, interview with the authors, November 23, 2022.

[23] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[24] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[25] Participant in workshop conducted by RAND and FOI, January 11, 2023.

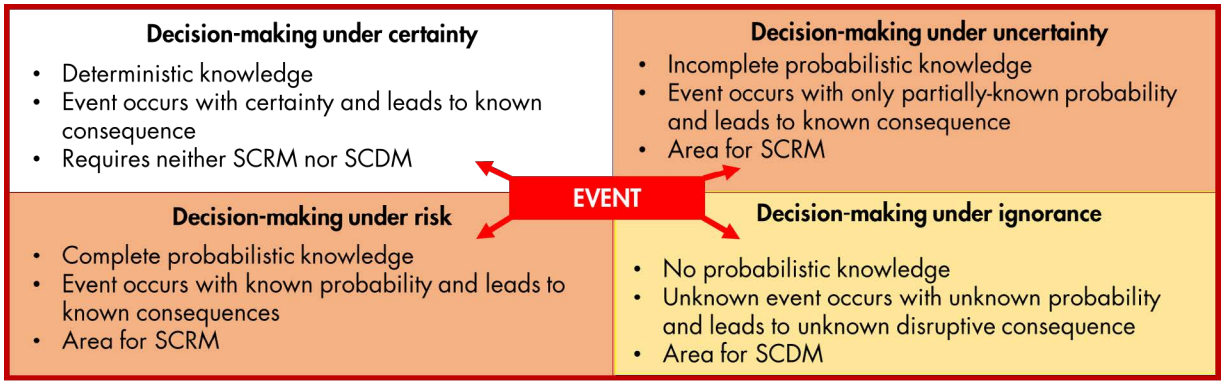
The variety and lack of predictability associated with recent supply chain disruptions have caused some experts to argue that SCRM is no longer sufficient and that, instead, more resilience-based thinking is needed.[26] To add to the debate, this project team proposes, in line with a few other academics, to use the term *SCDM* to describe how managers should think about addressing disruptive events (Dolgui and Ivanov, 2021; Altay and Pal, 2022). The next section explains SCDM as a distinct practice.

2.4. Features of Supply Chain Disruption Management

Having identified a gap in researchers' and practitioners' ability to better prepare for and mitigate the impact of unforeseen events, the project team argues that researchers and practitioners should address SCRES through the area of **SCDM—a new managerial activity** that is complementary to but distinct from SCRM. SCDM, therefore, is **dedicated to activities directed toward supply chain decisions under ignorance, the unknown unknowns, and disruptive events that are not successfully avoided through SCRM**. In the case of complete ignorance, decisionmakers have no knowledge of what these events are (even if their categories may be known), how likely they are to occur, when or where they might occur, or what consequences they might have if they occur. Furthermore, their impact cannot be quantified. The objective of SCDM is therefore to increase the resilience of a supply chain to any type of disruption—that is, to impart the supply chain with structural and control features that serve to quickly transition the supply chain to an acceptable—or even superior—state of functioning after a disruption about which there may have been no prior information (Ponis and Koronis, 2012).

In considering the four quadrants laid out in the previous section, two of the four quadrants can arguably be better addressed by SCRM. These quadrants are shaded orange in Figure 2.2. However, for the fourth quadrant, decisionmaking under ignorance, SCRM is insufficient to enhance SCRES. Therefore, SCDM is needed. This quadrant is shaded yellow.

Figure 2.2. Quadrants for SCRM Versus SCDM



SOURCE: FOI research based on Hansson (2005).

[26] Katsaliaki, Galetsi, and Kumar, 2021; Ali, Mahfouz, and Arisha, 2017; Nakano and Lau, 2020; participant in workshop conducted by RAND and FOI, January 11, 2023.

Using the term *SCDM* enables researchers and practitioners to explicitly distinguish disruption occurrence from disruption risk. Given the inability to guarantee the prevention of disruptions, there may be benefits to investing in SCRES using methods that are distinct from a SCRM approach.

Despite pandemics more broadly being included on numerous risk registers in the years before the COVID-19 pandemic, most societies in the world were not prepared for a pandemic. Additionally, given the range of potential pandemic scenarios (e.g., type of disease, method of transmission, starting point, international policy reactions, mitigation measures), it would have been nearly impossible to correctly quantify the likelihood or impact of this particular risk. Decisionmaking before the COVID-19 pandemic could therefore, under the definition used in this report, be classified as decisionmaking under ignorance; preparations would therefore fall under the category of SCDM.

As a result of the lack of knowledge prior to the pandemic, countries did not have sufficient stocks of the appropriate personal protective equipment (PPE), and industry lacked preparedness to increase production of PPE at short notice. Additionally, hospitals lacked sufficient equipment, including breathing apparatuses. When the pandemic struck, factories and distribution networks (e.g., harbors, airports) were shut down unexpectedly because of emergency policy measures and, eventually, a lack of personnel. Companies were therefore unprepared for massive increases in the cost of freight and for the significant growth in waiting times at key harbors and ports.

Effective SCDM that might have increased SCRES for an event similar to the COVID-19 pandemic might have included disaster-agnostic procedures for moving goods between harbors, stocking generic PPE, or making provisions to surge the capacity of hospitals or other medical care facilities at short notice. Mechanisms for coordinating between countries as emergency provisions were brought in, for example, are also an example of a relatively risk-agnostic procedure that might have helped coordinate supply chains shifting from one distribution node to another. An additional example of a successful SCDM practice during the COVID-19 pandemic is outlined in the following box.

DoD Response to COVID-19

In spring 2020, the worldwide spread of COVID-19 created massive disruptions to production in the U.S. defense industrial base (DIB). Pandemic-related shutdowns halted much production activity for several weeks.[a] While DoD quickly recognized the likely hazards that were posed to delay defense production activity, there remained substantial uncertainty over their likely severity. One serious concern revolved around the severe reduction of cash flow that vendors received from completing deliveries within both the defense and civilian sectors.[b] While firms could change their individual spending patterns to mitigate some of these challenges, the scale meant that effects were likely to only continue growing and were also likely to have long-term effects on the viability of firms in the U.S. DIB. To try to prevent this disruption, DoD took several steps, including providing over $2 trillion in funding to quickly route cash to firms in the DIB and reestablish cash flow through the completion of existing work. For this specific instance, the Coronavirus Aid, Relief, and Economic Security (CARES) Act provided the necessary mechanisms for providing loans, loan guarantees, debt relief, and other financial assistance.[c] For more information about how this and other policies helped to sustain the U.S. DIB, please see Wirth et al. (2021).

SOURCE: RAND research.

[a] DoD stated that 950 U.S. companies in the DIB closed for an average of two weeks in the spring of 2020; data from the Defense Contract Management Agency (DCMA) show that from the middle of March 2020 through the end of April, 106 out of 10,509 primary Pentagon contractors had to close—427 of the 11,413 subcontractors that DCMA tracks. DCMA points out that there were even more shutdowns deeper in the supply chain that were harder to track and quantify (Janes Intelligence Briefings, 2020; Hitchens, 2020).

[b] A survey conducted by the National Defense Industrial Association in late March 2020 revealed that "60% of respondents expect to have long-term financial and cash-flow issues as a result of this crisis" (Evans and Shanley, 2020).

[c] For more information about the specific mechanisms for increasing cash flow, please see Lopez (2020), Hitchens (2020), and Proujansky (2020).

Chapter 3

Nature of Defense Supply Chains and Implications for SCDM

The previous chapter discussed SCM in a relatively sector-agnostic manner. To some extent this is appropriate, because supply chains across all sectors share similar structures and properties. However, the unique nature of certain sectors entails a need to think specifically about SCRM, SCRES, and SCDM within the context of particular constraints and structures. This project team contends that defense is one of those sectors that must be considered within its own unique context. This chapter therefore sets out the reasons for that thinking and delves into some of the characteristics that distinguish defense supply chains from supply chains in other sectors.

3.1. Characteristics of Defense Supply Chains

For the purposes of this project and as discussed in section 1.3, *defense supply chains* refers to all of those supply chains that **are intended to provide military-specific supplies to ministries of defense and the armed forces of various countries**. The project team decided to use the term *commercial supply chains* to refer to **sectors outside of defense and outside of other government procurement**.[27] This section provides a brief overview of some of the important aspects of defense supply chains across their structures, characteristics, and challenges that distinguish them from their commercial counterparts. Of note, while not all of these individual factors are unique to defense supply chains, the combination makes defense supply chains a case that must be considered in its own context.

Defense and commercial supply chains are closely intertwined because both military equipment and logistics rely on commercial suppliers, materials, and products to varying degrees (Davis and Sullivan, 2017). Conversely, while some defense suppliers produce exclusively defense and military equipment, a number operate in both defense and commercial markets because their technologies and products have both civil and defense applications (i.e., dual-use products). At the same time, however, there are several crucial differences between defense supply chains and supply chains in other sectors; these differences are essential for the purpose of this project and for a more nuanced understanding of the challenges and opportunities for defense supply chains specifically.[28]

---

[27] Of note, while we are aware that commercial participants are heavily involved in defense supply chains, we have decided to use *public sector* or *government* versus *private sector* to distinguish between those participants in defense supply chains who work for businesses outside of government, as opposed to those supply chain practitioners and policymakers who work directly for the government.

[28] For additional discussion of supply chain design specifically for the defense sector, please see Ekström, Hilletofth, and Skoglund (2020).

Defense supply chains are designed to support the concentration and exercise of combat power. Defense supply chains are often used interchangeably with *military logistics*,[29] which can be defined as the "science of planning and carrying out the movement and maintenance of [armed] forces" (Osinga, 2016). However, supply is but one function of military logistics, which also includes functions as diverse as maintenance, engineering, and health services. Additionally, the project team's focus was on the industrial dimension of defense supply chains, and mainly the activities, processes, and products that are needed to produce and supply equipment (including ammunition and spare parts) from industrial facilities to ministries of defense. This meant that the project team did not specifically look at last-mile resupply, as discussed in section 1.3.[30]

Figure 3.1 broadly illustrates the structure of defense supply chains. It also identifies key areas of interest that will be discussed in this section, such as last-mile or tactical logistics, as well as the multiple tiers of suppliers that make up the DIB.

3.1.1. Structure of Defense Supply Chains

For some countries, most notably the United States, defense represents one of the few sectors in which government is the end customer. However, there are a number of additional structural factors that make defense supply chains unique. While in the broadest sense defense supply chains connect suppliers (industry) to customers (ministries or departments of defense) and end users (armed forces), just as their commercial counterparts do, the structures within which those connections take place are different for the defense sector compared with other sectors, in which the connections are largely business to business or directly from business to consumers. Specifically, there are several structural factors that distinguish defense supply chains from most commercial supply chains:

- The military parts of defense supply chains are often managed or overseen by **large complex government bureaucracies**.[31] While this can mean that funding and other resources to cover externalities and recover from disruptions can be marshalled because of the power of the state, the size of these bureaucracies often limits their agility and flexibility.[32] Defense contracting and procurement processes are also often complex, regulated, slow, long, and restrictive, making it difficult to adapt to sudden changes.[33]

[29] Interview B; Interview D, subject-matter expert, interview with the authors, November 23, 2022.

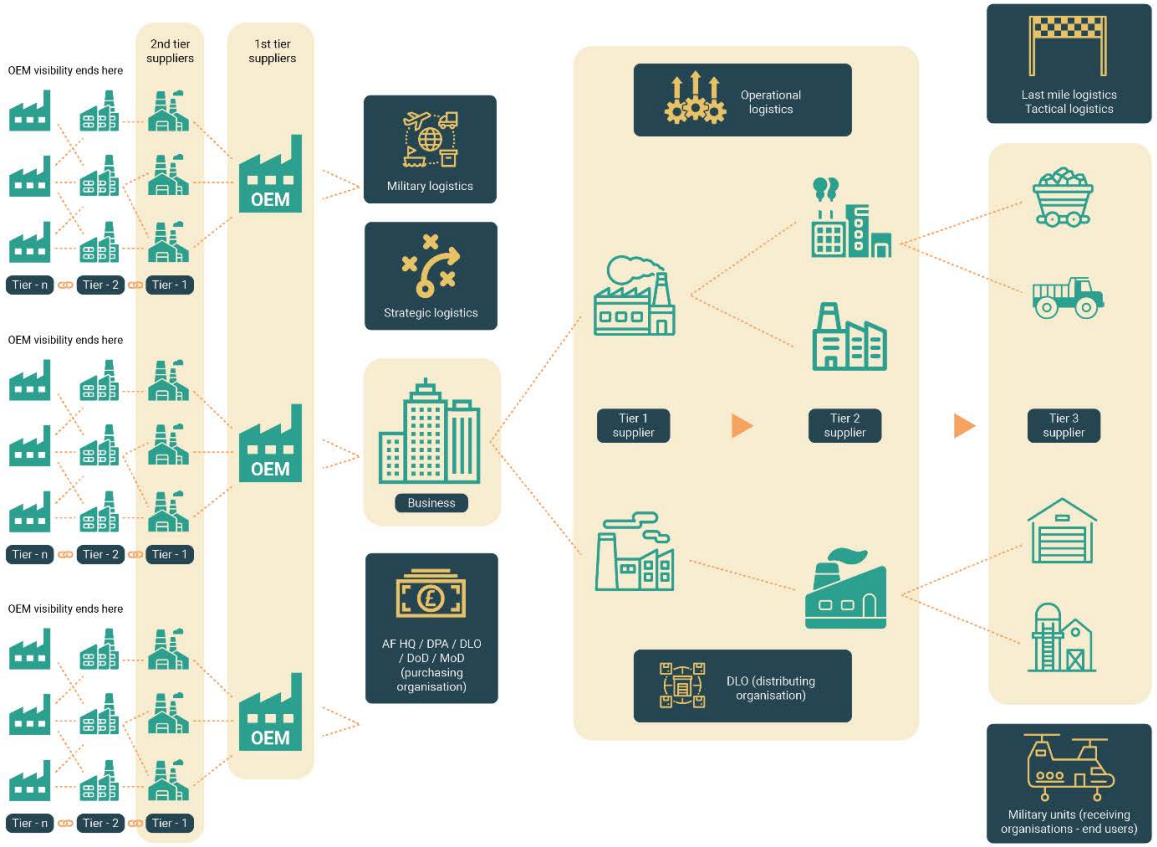
[30] The UK MOD defines *last-mile resupply* as "the delivery of combat supplies from the forward-most location (such as a physical base or a logistics/infantry vehicle) to personnel engaged in combat operations" (UK MOD, 2017).

[31] Interview D; Interview E, subject-matter expert, interview with the authors, November 24, 2022; Interview G, subject-matter expert, interview with the authors, November 16, 2022; Interview K, subject-matter expert, interview with the authors, November 16, 2022; participant in workshop conducted by RAND and FOI, January 11, 2023.

[32] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[33] Interview E; Interview K; Interview J; participant in workshop conducted by RAND and FOI, January 11, 2023.

Figure 3.1. Structure of Defense Supply Chains



SOURCE: FOI research.
NOTE: AF HQ = Armed Forces Headquarters; DPA = Defense Production Agency; DLO = Defense Logistics Organisation; MoD = United Kingdom Ministry of Defence; OEM = original equipment manufacturer.

- **Defense supply chains involve not only government departments but also a large number of private sector companies.** Public and private sector actors are responding to very different sets of incentives, imperatives, and requirements, which can make it difficult for all to cooperate or even share information or assign responsibility.[34] For example, the customer in defense supply chains (government) is often **constrained by unique regulations and requirements, including requirements for transparency and government scrutiny**, as a result of making purchases with the taxpayers' money. Additionally, the government customer in turn is subject to multiple conflicting pressures from its citizens or different political parties, especially within democracies.
- In many commercial supply chains, the end consumer who engages in a commercial transaction to procure the item in question is also the end user (Singh, Gupta, and Gunasekaran, 2018). In defense supply chains, these two functions are often separated: **End users have some but not always much influence in procurement and acquisition,** and their input can be diluted by intermediary procurement departments and officials. The demand signals therefore operate somewhat differently from the commercial market (Singh, Gupta, and Gunasekaran, 2018).
- Defense supply chains, similar to their commercial counterparts, consist of multiple tiers of contractors. In the first tier are prime contractors who deal directly with governments. They then contract out subcomponents to contractors in lower tiers, who then pass along discrete pieces of work to contractors in the tiers below them. These tiers are extremely difficult to map: A recent survey showed that most companies in the defense supply chain do not even know that they are part of that supply chain (Taylor and Lucas, 2020). This makes it particularly difficult to apply management practices, such as security guidance, throughout a supply chain.

3.1.2. Dynamics of Defense Supply Chains

Defense supply chains are dynamic and are often required to adapt to many different situations and operate under unique strains, particularly in times of geostrategic tensions, as demonstrated in the ongoing Russian war in Ukraine.[35] Defense supply chains have a unique raison d'être: to ensure that national militaries have what they need to perform their tasks and missions and to be prepared to both deter and, if needed, respond to enemy attacks. This creates a number of unique dynamics that can affect decisionmaking and cost-benefit analysis for defense supply chains. These include the following:

- Defense supply chains are characterized by **layered or complex customer requirements**, because defense products are often engineered to order following the specifications of either national or foreign governments (for export). In many cases, these requirements can come at the cost of efficiency in the commercial sense. Further costs can arise due to security requirements—for example, in terms of enhanced cybersecurity, physical security, specific

[34] Interview E; Interview G.

[35] Participant in workshop conducted by RAND and FOI, January 11, 2023.

requirements for facilities and personnel involved in the design, development, and manufacture of defense equipment. All these factors can make it less attractive for new companies to enter the defense market.[36]

- **Defense sales can sometimes represent a small portion of a private company's total volume of sales**, even for some traditional defense and aerospace companies; this can reduce the amount of leverage that the defense part of the business has to affect broader corporate decisionmaking.[37] This factor can be particularly difficult given the need for companies to comply with the layered or burdensome requests mentioned above; there may be a temptation for companies to leave the defense sector in favor of other types of business if requirements should grow too onerous.[38]
- Defense systems can have a **limited number of suppliers**, constituting an oligopoly, either because they supply niche capabilities or technologies or because of security requirements, resulting in an overall limited redundancy throughout the sector.
- Modern defense platforms and systems (e.g., armored vehicles, air defense systems) have **long life cycles**, which not atypically span several decades, increasing the uncertainty around security of supplies as time passes and conditions change, as well as the risk of obsolescence. For example, there is a concern that using small or medium enterprises as part of the supply chain may impact long-term availability of products and spare parts for the full life cycle of a system, because these companies may be acquired or may fold and thus would no longer be able to provide the required support for the defense equipment procured.[39]
- The **flow of goods between defense producers and end users is more often bidirectional** compared with commercial supply chains (in which goods flow from suppliers to retailers) because of corrective and preventive maintenance of defense equipment. This adds complexity but also means that there is a wide variety of goods flowing through defense supply chains at any one time, necessitating varying levels of specialist packaging and supporting infrastructure (Sokri, 2014). Additionally, this can create dependencies: If, for example, countries procure equipment from abroad, they need to either be able to import or export the systems to maintain their capabilities.[40]

3.1.3. Challenges for Defense Supply Chains

Perhaps the most important aspect of defense supply chains is that, given their intended purpose, the **cost of interruptions in the defense supply chain cannot be calculated in monetary terms.** Instead, the cost may amount to the loss of a key capability needed for deterrence or warfighting or may

[36] Interview B; Muravska et al., 2021. For more information on key challenges that small and medium enterprises face breaking into the defense industry, see Muravska et al. (2021).

[37] Interview G.

[38] Interview E.

[39] Interview G.

[40] Interview K.

have significant ramifications for loss of life.[41] The "worst-case" outcome of nonavailability of supplies can have "exponentially high costs" in the case of war and in terms of lives (Sethi and Sharma, 2018; Sokri, 2014). Therefore, even if the nonmonetized cost of a supply chain failure is known, it is almost impossible to balance this against the cost of mitigation measures. Additionally, the way in which successful management practices are measured is different because the overarching performance metric (particularly for government employees) is readiness for war, assured access, and assured supply rather than profit maximization.

Also, in contrast to most commercial supply chains, defense supply chains face a number of other challenges:

- **Wartime and operational conditions** are volatile, and conflicts can break out anywhere, without (much) warning, meaning that the nature or pace of demand for equipment can change suddenly and rapidly; the uniqueness of these conditions also makes it difficult to use them for the extrapolation of future vulnerabilities (Ryczynski and Tubis, 2021).
- Defense supply chains, particularly during instances of combat, are **more likely to be the subject of a targeted attack** than most commercial supply chains (Zhao et al., 2011).[42] These can be physical attacks or, equally as important, cyberattacks.[43] This creates a series of unique challenges that defense supply chains must consider regarding resilience or risk mitigation: One key example of this is the enhanced cybersecurity requirements that both the United States and the UK are putting in place for companies involved in the defense supply chain.[44]
- Given security concerns (e.g., sovereignty, freedom of action), **there are stronger drivers in defense than in other sectors for countries to secure their supply of equipment and ongoing support.** While not always possible, this is often attempted through sovereign development or procurement from allies and other trusted suppliers, both of which have the potential to sacrifice performance or increase cost to ensure supply or freedom of action.[45] Additionally, the need to "friend-shore" production to secure supply lines can also create additional integration challenges between equipment or requirements from diverse suppliers.[46]
- Decisions about the countries from which items can be sourced may not be driven by geographic convenience or cost but instead could be **based on geopolitical considerations** (e.g., trade sanctions or embargoes, concerns about reliability, political instability).[47] This can be particularly complicated for high-tech items for which there may only be a small number of suppliers or for open-source code for which the identities of the contributors are not always clear.

[41] While this is true for some commercial sectors, such as medical supply chains, it applies more uniformly across defense than for most other areas.

[42] This difference may not apply to supply chains that produce critical products, such as medicine or components for critical national infrastructure.

[43] Interview L.

[44] Taylor and Lucas, 2020; Interview L.

[45] Interview C, subject-matter expert, interview with the authors, November 22, 2022; Interview K

[46] Interview D; Interview G.

[47] Interview A, subject-matter expert, interview with the authors, November 21, 2022.

- Particularly during extended periods of peace without clear threats, **allocating spending for defense can be difficult in the face of competing priorities,** such as education, health care, and other government requirements. As governments try to allocate funding, given that SCDM and approaches that enhance resilience are often more expensive, "just-in-time" or "lean" approaches to SCM are often selected to meet budgetary targets.[48] While interviewees and workshop participants stated that this is changing following COVID-19 and the Russian invasion of Ukraine, the necessary changes take time to implement and to take effect.[49]

3.2. Observations on Supply Chain Disruption Management in Defense

The objectives, structure, and incentives of defense supply chains can differ significantly from commercial supply chains. Defense supply chains and their SCDM practices and approaches are therefore subject to a set of inherent constraints that are not present in commercial and business approaches to SCDM. While most of the literature on SCM focuses on the commercial sector, and there is a lack of literature on SCDM specifically, the project team was able to pull together information from those sources that do exist, as well as from consultations with practitioners and key stakeholders in the defense sector, in order to make certain observations about how SCDM is currently conducted in defense. As noted in Chapter 1, these observations do not represent a systematic review of the field but rather what the project team was able to gather within the constraints of this project; therefore, further research is needed to build a more comprehensive view.

Because of these distinctions, a number of key differences arise between defense and commercial SCDM practices and approaches. Interviewees emphasized that this means that the **SCDM practices and approaches available to defense are arguably more restricted** than those available to their commercial counterparts.[50] However, there is also arguably greater importance for SCDM in the defense sector than in more traditional commercial sectors, given the consequences of interruption and defense's purpose. For example, holding large stocks of inventory can be potentially perceived as an imperative given the costs of not having access to that inventory, more so than it might be for a commercial supply chain that could face lower profits if excess stocks are kept. Although shrinking defense budgets, new public management, and strong emphasis on value for money have often introduced more commercial approaches into defense logistics and into defense supply chains over the last few decades (e.g., just-in-time supply, lean approaches, reduced stockpiling), recent crises have encouraged a review of this logic and its applicability to defense and greater reflection on alternative approaches that will be more resilience-enhancing.

While there is limited evidence in academic literature on good practices in SCDM (with much focus placed on SCRM instead), interviews with practitioners conducted as part of this project provided some insight into emerging practices in SCDM in the defense context, as well as some of the inherent

[48] Ekström, Hilletofth, and Skoglund, 2020; participant in workshop conducted by RAND and FOI, January 11, 2023.

[49] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[50] Interview A; Interview G; Interview K; Interview L.

challenges accompanying those practices. This section is therefore intended to stimulate discussion of these practices and challenges. It does so by taking stock of some recent practices and approaches used by governments and defense companies to prepare for and mitigate disruptions, as well as the identified gaps in the design and implementation of these practices. Although no specific timelines on how long these practices have been in place were provided by the interviewees, many of them referred to COVID-19 as a key driver for the implementation or improvement of the below-mentioned defense SCDM practices.

3.2.1. Illustrative Examples of Current Practices in Defense SCDM

When asked about existing SCDM practices with relevance for defense supply chains, interviewees repeatedly reflected on the following practices:

- **Strengthened military logistics:** Several interviewees noted that preparedness against disruptions in the military is mostly driven by logistics.[51] Common practices include inventory buying, storing, monitoring and delivery, obsolescence management, warehouse positioning in line with operational planning, and day-to-day operation and maintenance of military infrastructures. However, such practices do not address the broader structural and networkwide concerns that this report seeks to understand.
- **Contractual supply chain protection:** According to three interviewees, government contractors are increasingly adding security provisions in procurement contracts to preempt supply chain disruptions.[52] Interviewees mentioned the benefits of recent updates to the UK MOD's Defense Conditions, including the requirement for prime contractors and their subcontractors to comply with strict cybersecurity measures, the new obligation for prime contractors to list the entirety of their subcontractors down to Tier 4[53] in order to provide the UK MOD with sufficient supply chain visibility, the obligation to ensure that the contractor is protected from hostile foreign takeovers, and the requirements for contractors to pay their subcontractors within a period of up to 30 days so as to avoid negative cash flows that would prevent subcontractors from delivering their services.[54]
- **Contractual agility:** One interviewee mentioned new initiatives to delegate supply chain decisionmaking to contractors to make sure that suppliers also have the tools to prepare against disruptions and adapt on the ground.[55] According to the interviewee, Germany has been increasingly offering contracts that allow companies to buy, increase, or change stocks based on their own assessment of the supply chains to enhance the resilience or cost-effectiveness of military logistics. The interviewee also noted that prime contractors are regularly contracted

[51] Interview D; Interview E; Interview K.

[52] Interview B.

[53] See Figure 3.1 for a diagram of the supply chain that includes the multiple tiers of contractors.

[54] Interview A.

[55] Interview E.

by the German Armed Forces to track materiel obsolescence and report their general logistics' resilience against disruptions.

- **Development and recruitment of supply chain units and personnel:** According to several interviewees, there have been efforts to create armed forces units dedicated to ensuring SCRES against disruptions. One interviewee mentioned the creation in Germany of a unit specifically dedicated to SCM within the Armed Forces' Center for Logistics, which is headed by the Joint Support Service.[56] Relatedly, another German interviewee emphasized efforts to recruit more supply chain experts and personnel who are tasked with day-to-day logistics and procurement management.[57] This interviewee mentioned about 10,000 civilians working at the German Department for Procurement and about 20,000 logisticians operating for the military, which reportedly is a high number in comparison with the number of active personnel in the German Armed Forces (about 180,000 active personnel in 2019).[58] In the UK, two stakeholders mentioned that the UK MOD pays particular attention to ensuring that defense contractors have sufficient supply chain skill pipelines to handle potential disruptions.[59]
- **Digitalization of supply chains:** Supply chains are increasingly digitalized to increase their resilience against disruptions. An interviewee cited the development in Germany of a 3D printing center and decentralized 3D printing capabilities that can be brought closer to the front line and can therefore bypass diverse supply chain disruptions, such as transportation disruptions or factory closures.[60] Smart warehousing systems are also effective tools with which to track inventory effectively and measure obsolescence.[61]
- **Predicting and testing resilience against disruptions:** Further to the digitalization of supply chains, several interviewees highlighted investments by governments and companies into big data analytics that are capable of generating cutting-edge simulations that can measure and predict the impact of disruptions.[62] One interviewee, in particular, mentioned ongoing work to develop an analytical tool that leverages geospatial capabilities to capture entire supply chains, including suppliers and resources, and to map risk levels to different risk categories (e.g., cyber disruptions) using predictive insight and historical data.[63] In parallel, disruption scenarios and associated resilience plans are being established by governments, though one German interviewee pointed to the lack of implementation of those scenarios in real-world operational environments.[64]

[56] Interview D.

[57] Interview E.

[58] The research team could not verify the accuracy of these estimates.

[59] Interview A.

[60] Interview E.

[61] Interview E.

[62] Interview E and Interview F, subject-matter expert, interview with the authors, December 2, 2022.

[63] Interview F.

[64] Interview E.

3.2.2. Persistent Challenges for SCDM for Defense Supply Chains

Several interviewees repeatedly mentioned a number of gaps in approaches and practices currently in place for managing defense supply chains that hamper effective SCDM.[65] First, when asked to pinpoint disruption scenarios against which defense is not sufficiently prepared, many stressed that global, externally generated disruption scenarios were particularly poorly addressed by current practices, in contrast with internal disruptions affecting day-to-day military logistics.[66] These scenarios include pandemics, natural disasters, national electrical blackouts, large-scale cyberattacks, and the inability to access microchip supplies. One interviewee even questioned the ability of their country's military to face a full-scale war that would mobilize the entirety of their defense industries given their primary focus on peacekeeping operations,[67] while another interviewee characterized the collapse of NATO as a major disruption for which their country would not be prepared.[68] Concerns about global, external disruptions mostly stem from interviewees' countries' dependence on other politically and economically unstable or unfriendly countries for the provision of critical supplies or their reliance on external military protection (e.g., NATO).

Specifically, a number of other cross-cutting gaps in approaches and practices were identified by the interviewees and workshop participants. While most of these appear in the research agenda, and are therefore discussed in detail in the next chapter, there were two additional gaps that did not fit neatly into categories:

- **Lack of understanding of the commercial components of the defense supply chain:** A recurring theme during the workshop was that current defense SCDM approaches still largely focus on the first few tiers of the defense supply chain, chiefly the prime contractor, and tend to overlook the commercial subcontractors involved in the upstream supply chains. Relatedly, many workshop participants argued that there is a general disregard for risks and disruptions that stem from commercial supply chains and affect the military buyer. They therefore called for more-holistic SCDM approaches and fostering collaboration between defense and commercial supply chain actors to better understand and mitigate weak links within upstream and downstream defense supply chains.
- **Absence of a recovery strategy within SCDM approaches:** A few interviewees and workshop participants observed that current SCDM approaches do not sufficiently focus on recovery, a key property of resilience that SCDM is trying to achieve.[69] *Recovery* is commonly defined as the ability of the supply chain to recover to the previous state.[70] One interviewee highlighted the fact that their country's defense ministry particularly struggles to learn from its mistakes and to adapt its approaches after a disruption has ended.[71] Given that recovery is a

[65] Interview A; Interview B; Interview D; Interview E; Interview G; Interview K; Interview L; Interview I; Interview J.

[66] Interview A; Interview D; Interview K; Interview L.

[67] Interview K.

[68] Interview G.

[69] Interview E; Interview I.

[70] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[71] Interview E.

key gap in SCDM approaches, the workshop participants were keen to stress that further research is required to identify the tools that could help facilitate faster recovery.

Chapter 4

Toward an Effective SCDM in Defense Supply Chains

This chapter provides an overview of key enablers for SCDM in defense supply chains as identified through a literature review, interviews with academics and practitioners, and a validation workshop with experts. These enablers also represent some of the key gaps in research that the study team has identified throughout this project and thus are areas in which, the project team believes, further research should be conducted to inform more-robust SCDM approaches for defense supply chains.

4.1. Understanding Supply Chains' Composition and Resilience

The defense sector is large and difficult to characterize in terms of the diverse assortment of supplies it encompasses. The size and scale of defense supply chains, their multiple tiers of contractors and subcontractors, the multiple tasks they are required to fulfill (e.g., long-term tank maintenance and upgrades versus the process of delivering ammunition to soldiers in the field), and the different types of entities involved (e.g., government ministries, private companies) mean that, overall, they are relatively poorly understood.[72]

Additionally, there are few practical case studies on the implementation of practices for SCRES, SCDM, and SCRM in the context of defense supply chains (or at least few that are documented in open sources).[73] This leaves potential gaps in terms of sharing best practices or better understanding instances in which commercial sector best practices may be applicable. Many efforts that have been undertaken primarily focus on the last mile of resupply[74] or on delivery of equipment to an area of operations rather than on the broader networks that provide supplies, particularly those with components upstream that are outside of the direct control of the public sector.[75]

Across a number of nations included in this study, there is also a lack of understanding of the manufacturers and suppliers that may provide crucial subcomponents to key systems.[76] Security vulnerabilities can often present themselves at these unmapped points in the supply chain (Lucas and Taylor, 2021). Additionally, the lack of a nuanced understanding of the supply chain makes it difficult to understand how the closure of an apparently small company might jeopardize the ability to receive

[72] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[73] Interview C.

[74] See Figure 3.1 for a diagram of the defense supply chain, including the position of last-mile resupply.

[75] Interview D.

[76] Participant in workshop conducted by RAND and FOI, January 11, 2023; Interview B.

spare parts for a key defense system.[77] Finally, this lack of understanding prevents an understanding of areas in which these subcomponents may overlap: Though NATO allies may purchase missiles from different manufacturers, multiple manufacturers may share a single sub-supplier for warheads or rockets, presenting a key bottleneck in the event that multiple countries require missiles at the same time.[78] This can also be a factor for repairs, particularly if that expertise does not exist in the country in which the equipment is based.[79]

Ministries of defense and prime contractors have developed a range of initiatives aimed at consistently mapping supply chains and their performance against identified risks and potential disruptions. The UK MOD, for example, has recently published its "Defence Supply Chain Strategy," laying out its approach to building resilience into its supply chains (United Kingdom Ministry of Defence Strategic Command, 2022). To support the objectives outlined in its strategy, the UK MOD has also been investing in tools to gather information on specific defense supply chains, including its main actors and key dependencies, and has been assigning risk profiles to frequent UK MOD contractors.[80] Information-sharing on the state of supply chains is also facilitated by the contractual obligation for all suppliers; in parallel, such defense contractors as BAE Systems and Lockheed Martin are also setting up their own due diligence databases to identify and map new subcontractors.[81]

However, despite the recognition that this information is needed, even in the UK a great deal of this information remains unknown or relies on companies self-reporting information that the UK MOD then has limited ability to verify.[82] Better mapping of supply chains is therefore needed to improve decisionmakers' understanding of how and where both endogenous and exogenous disruptions may occur and where vulnerabilities reside within the supply chains.

4.2. Applicability of Commercial Sector SCDM to the Defense Sector

This research showed a current disconnect, particularly in the available literature, but also among academics and practitioners, regarding the state of SCDM in the commercial sector and similar approaches in the defense sector. Despite defense supply chains' unique nature, there may be common interests, challenges, and overlaps between the defense and commercial sectors. Some interviewees were keen to stress that there are opportunities for defense supply chains to learn from and collaborate with commercial supply chains.[83] For instance, one interviewee indicated that the food manufacturing sector was an interesting case study for defense given its experience in implementing crisis management against disruptions.[84] Other examples may be drawn from the use of emerging technologies, such

[77] Interview E.

[78] Interview B.

[79] Interview G.

[80] Interview A.

[81] Interview A.

[82] Interview B.

[83] Interview A.

[84] Interview A.

as blockchain, to enhance supply chain transparency; other emerging technologies, such as artificial intelligence, have been used to identify and measure vulnerabilities or aspects of resilience.[85] Comparisons with other industries could also help to identify best practices or effective strategies that might be applicable in defense.

Additionally, given the close connections between defense and commercial supply chains, collaboration with commercial supply chains was regarded by most of the interviewees and workshop participants as essential for enabling a more holistic understanding of the range of disruptions that could affect defense.[86] Participants emphasized that it is important to continue to apply relevant findings from commercial sectors into defense where appropriate and to recognize overlapping interests. Further research is therefore necessary to capture practices in the commercial sector that have relevance for the defense sector and adapt or adopt them into defense.

4.3. Challenges Due to the Multisectoral Nature of Defense Supply Chains

As discussed in previous sections, defense supply chains not only cross through different countries and production sectors but also weave back and forth between public and private sector actors. All of these complexities raise questions about what level of control a government can or should have over its defense supply chain: Some countries, such as France, have chosen to have more direct control over companies in their defense supply chains than, for example, the UK.[87] Furthermore, there are questions about the degree to which different governments should collaborate, either to increase specialization or to enhance cooperation on major defense projects.[88]

Given the expense associated with building defense systems, many countries have chosen to work together in order to produce defense products together.[89] While this cooperation has existed for decades, the scale and frequency has increased dramatically in recent years. Often, for security reasons, countries choose to work with friends and allies, such as within the F-35 or Eurofighter Typhoon consortia. However, such cooperation can be complicated by the desire of different countries to dominate manufacturing, by conflicting requirements, or by concerns about maintaining access to key technologies.[90] The U.S. International Traffic in Arms Regulations, for example, often restrict the degree to which countries can repurpose or reconfigure equipment that includes U.S. technologies; they also mean that the U.S. government retains veto power over any exports that include those technologies.

Even where formal cooperation between governments does not occur, defense supply chains frequently cross national borders. A broad degree of stakeholder collaboration is therefore necessary to ensure that, for example, critical national infrastructure, such as transportation networks or utilities,

[85] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[86] Participant in workshop conducted by RAND and FOI, January 11, 2023; Interview E; Interview D.

[87] Interview K; participant in workshop conducted by RAND and FOI, January 11, 2023.

[88] Interview D; participant in workshop conducted by RAND and FOI, January 11, 2023.

[89] Interview E.

[90] Interview E.

remains available to defense manufacturers.[91] This involves information-sharing not only between governments and their industries but also between different governments.[92] Finland, Norway, and Sweden, for example, share security-of-supply agreements across the three countries; such approaches may be beneficial for more countries to adopt.[93] Other interviewees argued that the better solution would be for different countries to specialize and retain responsibility for a particular product or system.[94] However, this could raise questions about where expertise for repair and upgrades should reside because local ability to repair and upgrade is often crucial for effective defense equipment support.

In addition to international collaboration, it is important to note that the interconnections between the public and private sectors in defense supply chains mean that greater cooperation between government and industry will also be required to effectively implement strategies for SCDM. Participants at the workshop pointed out the reliance that this creates between government and the private sector, often with a relatively short list of prime contractors.[95] However, there was little consensus regarding how exactly that cooperation should be facilitated.

Multiple interviewees noted that their governments lacked a strategy for instances in which the government might wish to exercise more control or intervene in commercial markets to ensure defense SCRES in the event of an emergency.[96] An interviewee noted the underlying tension between achieving a lean supply chain through offshoring and growing requirements to onshore suppliers and industries.[97] While none of the interviewees called for a complete renationalization of suppliers and industries, two of them argued in favor of systematically making sure that defense has the local equivalents of international industries and suppliers so that there is a "national backup" to support the supply chain in case of a global disruption.[98]

Additionally, two interviewees discussed how the government and Tier 1 and 2 suppliers should manage their relationships with subcontractors to achieve wider SCDM objectives.[99] One interviewee notably questioned the propensity of U.S. federal agencies to establish one overarching contract with the prime contractor, who is then trusted with contracting the subcontractors and ensuring that they respect and meet the SCDM standards and objectives.[100] The same interviewee argued that the federal agencies should consider establishing direct contractual relationships with mid-tier suppliers to have better control over defense supply chains.[101] Another practitioner criticized the U.S. DoD's inclination to manage its relationships with its suppliers primarily through cost monitoring.[102] While many firms

[91] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[92] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[93] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[94] Interview D.

[95] Interview D; participant in workshop conducted by RAND and FOI, January 11, 2023.

[96] Interview B; Interview J.

[97] Interview J.

[98] Interviews K; Interview G.

[99] Interview I; Interview J.

[100] Interview J.

[101] Interview J.

[102] Interview I.

view increased costs as a symptom of a problem and will work with their suppliers to understand and solve the issue, DoD primarily views cost as an outcome in itself and the basis of competition between its suppliers. This, the interviewee argues, can lead to several types of issues with its suppliers, including burnout, resource attrition, unwillingness to work with DoD, and inefficacy in solving cost-related issues.

4.4. Distinguishing Between SCRM and SCDM Approaches in Defense

This research clearly distinguishes between SCRM, which mitigates risks that are at least partially understood, and SCDM, which aims to enhance overall resilience to respond to any disruptions, including those that are not anticipated. Further research is required into where SCRM and SCDM approaches might be appropriate, as well as how they might complement each other in defense supply chains. However, the risk-based approaches of SCRM will continue to create a strong draw for individuals looking to demonstrate efficacy and the value for money of their approaches.[103] The new UK "Defence Supply Chain Strategy," for example, communicates extensively about the need to identify risks and prepare for the resulting crises; however, this is a risk-based approach that, as discussed, does not constitute SCDM and cannot fully enhance resilience (United Kingdom Ministry of Defence Strategic Command, 2022). It is therefore important to understand not only where SCRM and SCDM can complement one another but also the spaces in which SCDM will remain relevant. This is because there will inevitably be disruptions that cannot be predicted or that SCRM was not able to fully mitigate and will therefore interrupt the functions of supply chains. For further delineation between SCRM and SCDM and the gaps and shortcomings of both, please see Chapter 2.

4.5. Adequate Resourcing as a Core Enabler of SCDM for Defense

Investing in the face of unknowns and counterfactuals is always a challenge: Should a disruption fail to manifest, it is easy to argue that the investment was misdirected or made in error. Then again, the same can be said for investment in armed forces in the first place or for most insurance premiums that organizations and individuals pay as a precaution against different events, such as fire. Implementing effective SCDM measures is therefore dependent on developing measures of resilience, finding ways to quantify flexibility, and perhaps implementing cultural change to ensure that SCDM is better understood across not only defense organizations but also the public sector bodies that provide their funding.[104]

Key performance indicators (KPIs) may be one way of demonstrating value for money. Workshop participants identified the amount of time that a supply chain takes to recover from an interruption as one potential KPI that may be useful in demonstrating the value of resilience and comparing the

[103] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[104] Interview L.

utility of different SCDM approaches. However, additional research is still required to determine how this or other indicators and metrics can best be measured and demonstrate its importance to key decisionmakers.[105]

Multiple interviewees and workshop participants pointed out that, in the country in which they work, creating flexibility and agility within defense organizations will require cultural change.[106] In addition, doing so may require embedding a level of understanding that it may be necessary to increase resourcing to enhance supply chain continuity.[107] However, cultural change also takes time.[108] Research and consensus-building will be required to identify these areas and demonstrate their importance to justify increased spending.

In addition to monetary resources, defense organizations and the private sector require qualified and experienced personnel to implement and manage their supply chains. Several participants identified a lack of such personnel as a key challenge for their defense organizations.[109] Others referred to capable personnel as their organization's most valuable asset.[110] However, in order to ensure that such personnel are available, they must be identified and then appropriately trained, deployed, and retained within organizations that conduct SCM.[111] Often, SCM requires expertise, either in contracting and procurement regulation or in different types of technologies.[112] It also requires intangible abilities, such as interpersonal skills, creativity, and flexible thinking.[113] Identifying and retaining these personnel across defense supply chains is therefore a key challenge.

There is also a limited understanding of how processes might be optimized to better enable appropriate contracting mechanisms for agile, flexible supply chains. Some interviewees argued that short-term procurement contracts and competitive bidding with contractors are unsuitable to address disruptions given the usual long timelines to identify alternative suppliers and contingency solutions in defense.[114] Instead, one of them called for long-term contracts that would enable governments to establish longer relationships with key suppliers in the form of partnerships and hence enable the establishment of joint contingency planning for disruptions.[115] Longer contracts would also ensure that governments constantly have sufficient resources, skills, and industrial sites to address large-scale disruptions. Further to changing the procurement strategy, one interviewee also emphasized that governments should set coherent strategies for buying and stocking key raw materials.[116] The interviewee

[105] Interview A; participant in workshop conducted by RAND and FOI, January 11, 2023.

[106] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[107] Participant in workshop conducted by RAND and FOI, January 11, 2023.

[108] Interview K.

[109] Interview G; Interview E; Interview A.

[110] Interview C.

[111] Interview A.

[112] Interview G.

[113] Interview E.

[114] Interview K; Interview J.

[115] Interview K.

[116] Interview E.

notably cited the example of the U.S. government, which is currently buying multiple raw materials (e.g., fuel) for its strategic agility reserves.

Chapter 5

Research Agenda to Support Effective SCDM for Defense

Building on the previous chapters, this final chapter presents a number of overarching findings from this research project before detailing a research agenda intended to support and encourage further research into defense SCDM.

5.1. Overarching Observations

Though the primary purpose of this research project was to design an agenda to guide research for defense supply chains' ability to deal with disruptive events, the literature review, interviews, and workshop also produced additional observations that run throughout the findings detailed in the previous chapters. Because of the limited time and resources available for this project, these are not exhaustive or conclusive; however, the project team hopes that they will be taken forward and developed in future research projects.

First, the research found that across both defense and commercial sectors, organizations and individuals are becoming increasingly aware that **21st-century supply chains are extremely vulnerable**. Interruptions to supply chains can originate both exogenously and endogenously to these vast supply networks, which all cross numerous sectors of business, as well as geographic and political boundaries. Some of these interruptions are caused by events that can be forecast, tracked, and measured and whose likely impact can be quantified; however, others are the result of disruptions that are unforeseeable and whose likelihood and impact cannot be quantified. Such disruptions may have a variety of origins, such as unanticipated demand surges due to war, unpredictable natural disasters, climate change, political turmoil, or malicious activity.

Despite an increasing ability to forecast and measure risks, unknown and unanticipated disruptions will always remain a threat to supply chains. For this reason, **supply chains will need to be resilient and able to absorb the impact of disruptions and regain functionality** when interruptions inevitably occur. This resilience needs to be event agnostic and therefore **cannot be gained through traditional risk-based SCRM approaches**. Instead, **the approach of SCDM may be increasingly required** to ensure that supply chains can continue to deliver their products in the face of unknown threats.

While SCDM is important across all sectors, it is particularly necessary for defense supply chains, where the costs of interruption are not primarily monetary. Instead, **disrupted defense supply chains can have national security implications**, affecting militaries' abilities to deter future aggression and to defend against adversaries. However, little research has been done into SCDM in the defense sector; much of the extant research has been conducted in commercial sectors that often have different

structures, characteristics, and challenges. Therefore, further research is needed to better understand how SCDM can be better implemented within the context of defense.

Given some of the peculiarities of the defense sector, there are **particular challenges that practitioners in both the public and private sectors will need to navigate**, including the following:

- **fostering better public-private cooperation on SCDM** between the companies that manufacture and supply defense supplies and the defense organizations that develop requirements for and subsequently purchase that equipment
- **adopting collaborative approaches to SCDM** that enable the sector as a whole to tackle challenges that would be impossible for companies or armed forces to handle in isolation
- **working toward international approaches to SCDM** that can better address the sprawling, multinational and multisectoral spread of many defense supply chains
- **identifying KPIs and other metrics** that can be used to quantify and understand the existing performance of supply chains in this area, as well as changes and improvements proposed through further research.

Further research across all of these areas is required not only to understand SCDM more generally but also to determine how it can best be applied for defense supply chains. The research agenda in the next section seeks to provide ideas for key questions that need to be better investigated in this space.

5.2. Research Agenda

The core purpose of this project has been to produce a research agenda to support robust research and analysis on defense supply chains and their ability to adapt and respond to unpredictable events and disruptions. Drawing on the findings of the research captured in Chapters 2, 3, and 4, this section presents the research agenda itself, exposed to and validated by experts in the field by means of a virtual workshop held in January 2023.

The following research agenda is divided into five sections corresponding to the key enablers for defense SCDM, as detailed in Chapter 4. While this agenda is by no means exhaustive, it pinpoints some of the most pressing and important questions in the field. To highlight those key questions further, the workshop included a prioritization exercise in which participants were asked to identify the top five questions. Bolded questions in this section were the most highly rated as a result of that exercise and were identified by three or more participants as among the most important for future research.

5.2.1. Improved Understanding of Supply Chain Disruptions in Defense Supply Chains

The research repeatedly showed that defense supply chains have unique needs and challenges depending on the sectors that they cross, the stakeholders they involve, and the nature of the end products. Broader theoretical questions are important for understanding the scope of disruption management; a more detailed understanding of the defense supply network as a whole and individual defense

supply chains requires specific investigation to understand the most effective approach to SCDM. Specific research questions in this area might include the following:

- What tools, techniques, and methodologies can governments and companies use to better understand and monitor their defense supply chains, including the multiple tiers of subcontractors?
- What risks and vulnerabilities are specific to defense supply chains or exist across multiple defense supply chains?
- How are SCRES requirements affected by the different ways that governments evaluate the costs of defense supply chain disruptions? How might these implications be different during a time of geopolitical conflict, such as war?
- What replicable examples of good practice have been used in defense supply chains that might be applicable to other defense or commercial supply chains?
- How can governments ensure that private sector suppliers in defense supply chains have the key tools needed to conduct SCDM and enhance SCRES?
- To better understand SCRES, how is *recovery* defined? Can time to recovery be measured?

5.2.2. Applicability of Commercial Sector Approaches to SCDM in Defense Supply Chains

As discussed previously, the research showed many differences between defense and commercial supply chains in terms of their structure, their nature, and the implications of disruption. A key gap identified is the ways in which disruption management approaches and strategies generated for commercial supply chains might or might not apply to the unique characteristics of the defense sector. Specific research questions in this area include the following:

- How can commercial supply chain disruptions impact their defense sector counterparts?
- What is the appropriate role of government in SCDM for the commercially owned segments of defense supply chains, given the unique requirements of defense supply chains?
- How do the differences between defense and commercial supply chains impact the relevance of commercial sector approaches? Are any commercial sector SCDM approaches appropriate or beneficial given the unique requirements of defense?

5.2.3. Challenges for SCDM from the Multisectoral Nature of Defense Supply Chains

Supply chains in both the commercial and defense sectors often have global reach and dependencies on diverse areas of national infrastructure (e.g., energy, transportation, communications, or banking networks). Therefore, the research suggests that effective defense SCDM may involve an industry-wide, nationwide, or even multinational approach. Given the national security implications of disrupting defense supply chains, this could be an area for government intervention; however, there is no consensus on the appropriate nature and extent of such intervention. Specific research questions in this area might include the following:

- **What approaches or tools can governments use to better collaborate with partners and allies to enhance the resilience of international defense supply chains or limit defense supply chains' exposure to potential adversaries (e.g., offshoring/ally-shoring)? What are the limits of this collaboration?**
- **What are some of the current enablers and barriers to cooperation between the private and public sectors in terms of defense SCDM?**
- To what extent might SCDM approaches in defense connect to broader discussions of societal resilience?

5.2.4. Distinguishing Between Risk Management and Disruption Management Approaches in Defense

The research clearly distinguishes between SCRM, which mitigates risks that are at least partially understood, and SCDM, which aims to enhance overall resilience to respond to unanticipated disruptions. Further research is required into where SCRM and SCDM approaches might be appropriate, as well as how they might complement each other in defense supply chains. Specific research questions in this area might include the following:

- **What further distinctions can or should be drawn between SCRM and SCDM to better enable defense practitioners across industry and government to address both areas?**
- In a defense-specific context, what are the respective strengths and weaknesses of SCRM and SCDM?
- Can SCRM and SCDM approaches complement one another in enhancing defense SCRES? If so, how?

5.2.5. Resourcing and Prioritizing Defense Supply Chain Disruption Management

The research confirms that a drive for lean or efficient approaches to SCM may have detrimentally affected SCRES. Despite the recognition of the importance of resilient supply chains, the financial constraints that drove these lean and efficient approaches are unlikely to abate. Supply chain professionals may therefore need to be able to demonstrate the need for SCRES and the value for money of SCDM. Specific research questions in this area might include the following:

- **What are some of the current or anticipated barriers and enablers for resourcing and implementing SCDM approaches in defense across different actors (e.g., government, private sector)?**
- **What are the key resources needed by practitioners in both government and the private sector to design and implement SCDM strategies in defense?**
- **What kinds of KPIs can be used to measure the performance of SCDM approaches in defense? How can the value for money of different approaches be demonstrated or understood in defense?**

It is the project team's hope and ambition that this research agenda will help support and encourage further inquiry in this key area for defense supply chains, be it by academics, practitioners, government, or private sector stakeholders, including defense industry, national ministries of defense and armed forces, and the traditional defense and security policymaking community.

Appendix A

Stand-Alone Research Agenda

This version of the research agenda is intended to stand independently from the broader report. It contains a shorter version of the research context and purpose, as well as the research questions.

A.1. Project Context and Purpose

RAND and the Swedish Defence Research Agency (Totalförsvarets forskningsinstitut; FOI) have been commissioned by the RAND Center for Global Risk and Security to set out a research agenda to help build understanding of how defense supply chains can better withstand severe, unanticipated disruptions (sometimes referred to as *black swans*[117] or *unknown unknowns*[118]). Many current approaches, both in the commercial[119] and defense sectors, are concerned with the mitigation of risks whose probability and impact can be at least estimated (known unknowns), which is addressed through more traditional supply chain risk management (SCRM).

However, though the likelihood of unknown unknowns is often perceived to be quite low (e.g., one-in-100-year events), recent years have seen global supply chains frequently disrupted across multiple sectors. Because the probability and impact of unknown unknowns are by definition impossible to calculate, the increasing number of such events has raised interest in enhancing supply chain resilience (SCRES) in order to mitigate their impact. In this study, we have drawn a distinction between SCRM, which addresses events whose probability and impact can be calculated or estimated, and supply chain disruption management (SCDM), or efforts to mitigate these unknown unknowns through enhancing SCRES.

Despite increasing interest in SCRES, SCDM remains an understudied area, particularly for supply chains in the defense sector. The research shows that defense supply chains have unusual characteristics, such as the relatively high level of government interference given the monopsonic nature of

[117] Popularized by Nicholas Nassim Taleb, *black swan events* are categorized as rare events whose likelihood is difficult or impossible to assess (Taleb, 2017). A black swan event is often characterized by three main attributes: The event is an outlier that sits outside of regular expectations; its consequences have extreme impacts; and it is only predictable in retrospect (Olivares-Aguila and Vital-Soto, 2021).

[118] The concept of *unknown unknowns* was popularized by Donald Rumsfeld in his famous 2002 remarks (U.S. Department of Defense, 2002). This project related Rumsfeld's three categories to the Johari window to establish four quadrants of decisionmaking: decisionmaking under certainty (known knowns), decisionmaking under uncertainty and risk (unknown knowns and known unknowns), and decisionmaking under ignorance (unknown unknowns) (Luft and Ingham, 1955).

[119] For the purposes of this document, *commercial* here refers to supply chains where the end consumer is outside of the defense sector. While the project team recognizes that the private sector and commercial companies are intimately involved in defense supply chains, they believed that this was the best way to delineate the defense sector as opposed to other areas that, for example, feed into industrial or consumer markets.

the market. In addition, their disruption also brings unique consequences, as they not only carry monetary costs but also have national security implications.

Further research is therefore required to determine how to define good strategies for SCDM, as well as how they might be implemented by stakeholders across both the private sector and government to enhance SCRES. This study therefore sought to help direct future research into SCDM for defense supply chains by setting out a research agenda in the following key areas.

A.1.1. Improved Understanding of Supply Chain Disruptions in Defense Supply Chains

The research repeatedly showed that defense supply chains have unique needs and challenges depending on the sectors that they cross, the stakeholders they involve, and the nature of the end product. Broad, theoretical questions are important for understanding the scope of disruption management. A more detailed understanding of the defense supply network as a whole and individual defense supply chains requires investigation to understand the most effective approach to SCDM. Specific research questions in this area might include the following:

- What risks and vulnerabilities are specific to defense supply chains or exist across multiple defense supply chains?
- How are SCRES requirements affected by the different ways that governments evaluate the costs of defense supply chain disruptions? How might these implications be different during a time of geopolitical conflict, such as war?
- What tools, techniques, and methodologies can governments and companies use to better understand and monitor their defense supply chains, including the multiple tiers of subcontractors?
- What replicable examples of good practice have been used in defense supply chains that might be applicable to other defense or commercial supply chains?
- How can governments ensure that private sector suppliers in defense supply chains have the key tools needed to conduct SCDM and enhance SCRES?
- To better understand SCRES, how is *recovery* defined? Can time to recovery be measured?

A.1.2. Applicability of Commercial Sector Approaches to SCDM in Defense Supply Chains

As discussed above, the research showed many differences between defense and commercial supply chains in terms of their structure, nature, and the implications of disruption. A key gap identified is the ways in which disruption management approaches and strategies generated for commercial supply chains might apply to the unique characteristics of the defense sector. Specific research questions in this area include the following:

- How can commercial supply chain disruptions impact their defense sector counterparts?
- What is the appropriate role of government in SCDM for the commercially owned segments of defense supply chains, given the unique requirements of defense supply chains?

- How do the differences between defense and commercial supply chains impact the relevance of commercial sector approaches? Are any commercial sector SCDM approaches appropriate or beneficial, given the unique requirements of defense?

A.1.3. Challenges for SCDM from the Multisectoral Nature of Defense Supply Chains

Supply chains in both the commercial and defense sectors often have global reach and dependencies on diverse areas of national infrastructure (e.g., energy, transportation, communications, or banking networks). Therefore, the research suggests that effective defense SCDM may involve industry-wide, nationwide, or even multinational approaches. Given the national security implications of disrupting defense supply chains, this could be an area for government intervention; however, there is no consensus on the appropriate nature and extent of such intervention. Specific research questions in this area might include the following:

- What are some of the current enablers and barriers to cooperation between the private and public sectors in terms of defense SCDM?
- How can governments better collaborate with partners and allies to enhance the resilience of international defense supply chains or limit defense supply chains' exposure to potential adversaries (e.g., offshoring/ally-shoring)? What are the limits of this collaboration?
- To what extent might SCDM approaches in defense connect to broader discussions of societal resilience?

A.1.4. Distinguishing Between Risk Management and Disruption Management Approaches in Defense

The research clearly distinguishes between SCRM, which mitigates risks that are at least partially understood, and SCDM, which aims to enhance overall resilience to respond to and recover from unanticipated disruptions. Further research is required into where SCRM and SCDM approaches might be appropriate, as well as how they might complement each other in defense SCM. Specific research questions in this area might include the following:

- What further distinctions can or should be drawn between SCRM and SCDM to better enable defense practitioners across industry and government to address both areas?
- In a defense-specific context, what are the respective strengths and weaknesses of SCRM and SCDM?
- Can SCRM and SCDM approaches complement one another in enhancing defense SCRES? If so, how?

A.1.5. Resourcing and Prioritizing Defense SCDM

The research confirms that a drive for lean or efficient approaches to SCM may have detrimental effects for SCRES. Despite the recognition of the importance of resilient supply chains, the financial

constraints that drove these lean and efficient approaches are unlikely to abate. To the extent that supply chain leanness degrades SCRES, supply chain professionals may therefore need to be able to demonstrate the need for SCRES and the value for money of SCDM. Specific research questions in this area might include the following:

- What are some of the current or anticipated barriers and enablers for resourcing and implementing SCDM approaches in defense across different actors (i.e., government, private sector)?
- What are the key resources needed by practitioners in both government and the private sector to design and implement SCDM strategies in defense?
- What kinds of key performance indicators can be used to measure the performance of SCDM approaches in defense? How can the value for money of different approaches be demonstrated or understood in defense?
- It is the project team's hope and ambition that this research agenda will help support and encourage further inquiry in this key area for defense supply chains, be it by academics, practitioners, government, or private sector stakeholders, including defense industry, national ministries of defense and armed forces, and the traditional defense and security policymaking community.

References

Luft, Joe, and Harry Ingham, "The Johari Window, a Graphic Model of Interpersonal Awareness," *Proceedings of the Western Training Laboratory in Group Development*, 1955.

Olivares-Aguila, Jessica, and Alejandro Vital-Soto, "Supply Chain Resilience Roadmaps for Major Disruptions," *Logistics*, Vol. 5, No. 4, 2021.

Appendix B

Study Methodology

B.1. Literature Review Strategy

The literature review was conducted with support from RAND Knowledge Services. Using the parameters provided by the research team, Knowledge Services identified 24 search strings. These search strings were used in Web of Science for English language sources between 2012 and September 2022. Search strings are available upon request.

B.2. Interviews

A small number of subject-matter expert interviews were conducted to help elucidate gaps that may have been left by the literature review. These interviews were conducted by all members of the study team across a variety of countries and institutions. In addition to speaking with academics, the research team took care to include a number of practitioners among the pool of interviewees. Some interviews involved multiple individuals. In total, 16 individuals were interviewed across 12 interviews. All interviews were conducted from November 16, 2022, through December 5, 2022.

B.2.1. Interviewee Affiliations

Interviewees were affiliated with the following organizations (Table B.1). Every effort has been made to anonymize their responses in order to ensure open and honest discussion.

Table B.1. Organizational Affiliations of Interviewees

Organization	Country
ADS Group	United Kingdom
Bundeswehr University Munich	Germany
International Centre for Defence and Security	Estonia
UK MOD	United Kingdom
Michigan State University	United States
The Norwegian Defence University College	Norway
The Swedish Defence University	Sweden
University of Missouri–St. Louis	United States
University of Vermont	United States
DoD	United States

B.2.2. Interview Protocol

The questions below were asked by all interviewers in a semistructured format.

Topic 1: How well developed are existing approaches to the problem of supply chain disruptions?

- What types of supply chain disruptions are most concerning to your organization?
- What practices are used in your organization for managing supply chain disruptions?
- Do you find there is general agreement on which practices to use and how to implement them? Are there specific areas where the choice of approach or method of implementation is uncertain or contentious?
- What resources does your organization use to manage supply chain disruptions? Some types of resources to consider might include
  - doctrine (institutional agreement on what to do)
  - personnel and their qualifications/training
  - organizational structure
  - policy and authority
  - data for measure supply chain disruptions and their consequences
  - funding.
- Is general agreement on the resources needed to implement current practices?

Topic 2: Are there disruption scenarios for which existing approaches are ill suited?

- What types of disruption scenarios are current practices intended to address?
- How effective are current practices for the types of supply chain disruption scenarios they are intended to address?
- Are there important disruption scenarios current practices are not intended to address?
- For these supply chain disruption scenarios, where do current practices work well and where do they not work well?
- What do you think might be the main reasons why current approaches do/do not work well against these disruption scenarios?
- What do you think might be most helpful for improving the resilience of defense supply chains against these disruption scenarios?
- Are current practices equally effective for defense and commercial supply chains?

Topic 3: What are the greatest barriers to better defense supply chain resilience practices?

- What do you think may be the biggest barriers for defense policymakers/decisionmakers in investing in approaches to improve supply chain resilience to disruption?
- Are there sources or types of information or research that you or your organization have found helpful in your practice?
- What additional research is needed to improve defense supply chain resilience? What do you need to know more about that you haven't run across in existing knowledge sources?

B.3. Workshop

This workshop convened primarily academics but also some practitioners to validate the research agenda generated through the literature review and interviews conducted to date for this project. The agenda (see section B.3.2) was shared with participants in advance for awareness and served as the basis of the Mural board (see section B.3.3) underpinning the workshop. The workshop was facilitated by RAND Europe and took place virtually on Wednesday, January 11, 2023.

B.3.1. Workshop Participant Affiliations

The workshop was conducted under a set of rules intended to preserve anonymity and enable free and open discussion. Therefore, no responses have been linked with particular individuals. However, the organizations with representatives at the workshop are listed in Table B.2.

Table B.2. Affiliations of Workshop Participants

Organization	Country
Bundeswehr University Munich	Germany
Chalmers University	Sweden
Cranfield University	United Kingdom
FOI	Sweden
Lancaster University	United Kingdom
The Norwegian Defence University College	Norway
Oregon State University	United States
RAND	United States
RAND Europe	United Kingdom; Belgium
The Swedish Defence University	Sweden
University of Southern Denmark	Denmark

B.3.2. Workshop Agenda

1400–1415 GMT: Intro and purpose of the workshop

- *RAND Europe to deliver with input from Thomas and Liz*

1415–1500 GMT: Research gaps

- *RAND Europe to facilitate discussion and control Mural*

1500–1510 GMT: Break
1510–1555 GMT: Research questions

- *RAND Europe to facilitate discussion and control Mural*

1555–1600 GMT: Break

- *Link to Mural to be sent around in the break to all participants*

1600–1615 GMT: Prioritization of research questions

- *All have access to Mural and will be given five minutes to put stickers on those research questions that they believe to be most important to address. Once the stickers have been placed, there will be a brief opportunity to ask questions about any anomalies or surprises.*

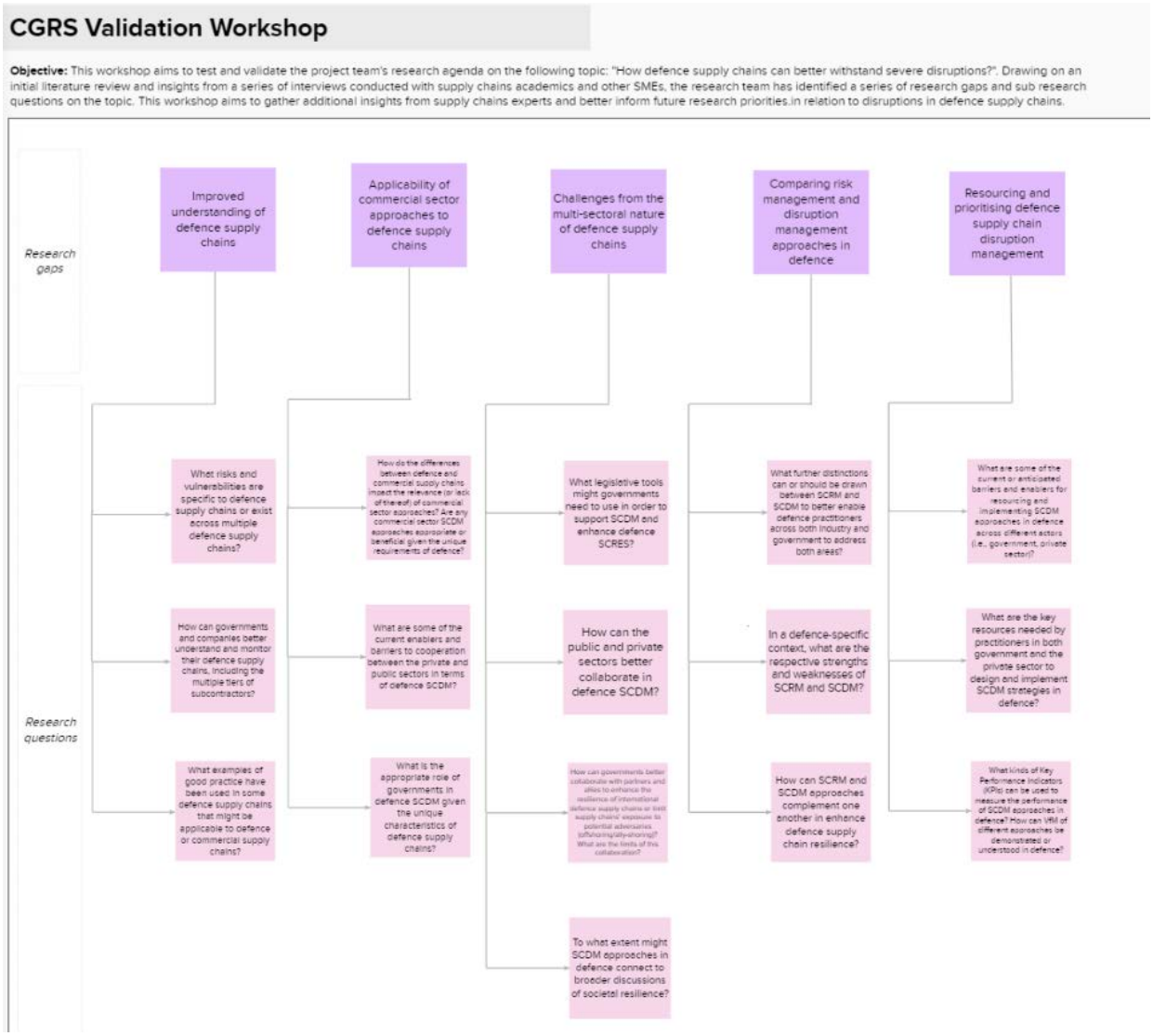
1615–1630 GMT: Close

- *RAND Europe to summarise proceedings, provide information on next steps and thank participants.*

B.3.3. Mural Board

The Mural board shown in Figure B.1 was used in the validation workshop to garner feedback from participants regarding the draft research agenda. The Mural board includes all questions from the draft research agenda, each under the heading of five primary research gaps.

Figure B.1. Mural Board



SOURCE: RAND and FOI research presented via the Mural platform.

Abbreviations

COVID-19	coronavirus disease 2019
DCMA	Defense Contract Management Agency
DIB	defense industrial base
DoD	U.S. Department of Defense
FOI	Totalförsvarets forskningsinstitut (Swedish Defence Research Agency)
KPI	key performance indicator
NATO	North Atlantic Treaty Organization
PPE	personal protective equipment
SCDM	supply chain disruption management
SCM	supply chain management
SCRES	supply chain resilience
SCRM	supply chain risk management
UK MOD	United Kingdom Ministry of Defence

Bibliography

Aboagye, Aaron, Ondrej Burkacky, Abhijit Mahindroo, and Bill Wiseman, "When the Chips Are Down: How the Semiconductor Industry Is Dealing with a Worldwide Shortage," World Economic Forum, February 9, 2022.

Ali, Abubakar, Amr Mahfouz, and Amr Arisha, "Analysing Supply Chain Resilience: Integrating the Constructs in a Concept Mapping Framework via a Systematic Literature Review," *Supply Chain Management*, Vol. 22, No. 1, 2017.

Altay, Nezih, and Raktim Pal, "Coping in Supply Chains: A Conceptual Framework for Disruption Management," *International Journal of Logistics Management*, Vol. 32, No. 2, 2022.

Anuat, Edward, Douglas L. Van Bossuyt, and Anthony Pollman, "Energy Resilience Impact of Supply Chain Network Disruption to Military Microgrids," *Infrastructures*, Vol. 7, No. 1, 2022.

Aqlan, Faisal, and Sarah S. Lam, "Supply Chain Risk Modelling and Mitigation," *International Journal of Production Research*, Vol. 53, No. 18, 2015.

Bier, Tobias, Anne Lange, and Christoph H. Glock, "Methods for Mitigating Disruptions in Complex Supply Chain Structures: A Systematic Literature Review," *International Journal of Production Research*, Vol. 58, No. 6, March 2020.

Brindley, Clare, and Bob Ritchey, "Introduction," in Clare Brindley, ed., *Supply Chain Risk*, Ashgate, Farnham, 2004.

Bui, Tat-Dat, Feng Ming Tsai, Ming-Lang Tseng, Raymond R. Tan, Krista Danielle S Yu, and Ming K. Lim, "Sustainable Supply Chain Management Towards Disruption and Organizational Ambidexterity: A Data Driven Analysis," *Sustainable Production and Consumption*, Vol. 26, 2021.

Chen, Injazz J., and Antony Paulraj, "Towards a Theory of Supply Chain Management: The Constructs and Measurements," *Journal of Operations Management*, Vol. 22, No. 2, 2004.

Chopra, Sunil, and ManMohan S. Sodhi, "Managing Risk to Avoid Supply-Chain Breakdown," *MIT Sloan Management Review*, October 15, 2004.

Christopher, Martin, and Helen Peck, "Building the Resilient Supply Chain," *International Journal of Logistics Management*, Vol. 15, No. 2, 2004.

Christopher, Martin, Helen Peck, and Denis R. Towill, "A Taxonomy for Selecting Global Supply Chain Strategies," *International Journal of Logistics Management*, Vol. 17, No. 2, 2006.

CNBC, "Gatwick Drone Disruption Cost EasyJet Nearly $20 Million," January 22, 2019.

Craighead, Christopher W., Jennifer Blackhurst, M. Johnny Rungtusanatham, and Robert Handfield, "The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities," *Decision Sciences*, Vol. 38, No. 1, 2007.

Davis, James, and John Sullivan, "Supply Chain Risk—What Is It?" *Defense AT&L*, March–April 2017.

Dolgui, Alexandre, and Dmitry Ivanov, "Ripple Effect and Supply Chain Disruption Management: New Trends and Research Directions," *International Journal of Production Research*, Vol. 59, No. 1, 2021.

Dolgui, Alexandre, Dmitry Ivanov, and Maxim Rozhkov, "Does the Ripple Effect Influence the Bullwhip Effect? An Integrated Analysis of Structural and Operational Dynamics in the Supply Chain," *International Journal of Production Research*, Vol. 58, No. 5, 2019.

Dolgui, Alexandre, Dmitry Ivanov, and Boris Sokolov, "Ripple Effect in the Supply Chain: An Analysis and Recent Literature," *International Journal of Production Research*, Vol. 56, No. 1–2, 2018.

Duong, Linh Nguyen Khanh, and Josephine Chong, "Supply Chain Collaboration in the Presence of Disruptions: A Literature Review," *International Journal of Production Research*, Vol. 58, No. 11, 2019.

Ekström, Thomas, Per Hilletofth, and Per Skoglund, "Differentiation Strategies for Defense Supply Chain Design," *Journal of Defence Analytics and Logistics*, Vol. 4, No. 2, 2020.

Evans, Corbin, and Camilla Shanley, *NDIA COVID-19 Small-Business Impacts Survey Summary*, National Defense Industrial Association, April 23, 2020.

Ferry, Heath, and Van Poindexter, "Supply Chain Risk Management: An Introduction to the Credible Threat," *Defense AT&L*, Special Section, 2016.

Golan, Maureen S., Laura H. Jernegan, and Igor Linkov, "Trends and Applications of Resilience Analytics in Supply Chain Modelling: Systematic Literature Review in the Context of the COVID-19 Pandemic," *Environment Systems and Decisions*, Vol. 40, 2020.

Handfield, Robert B., and Ernest L. Nichols, *Introduction to Supply Chain Management*, Prentice-Hall, 1999.

Hansson, Sven Ove, *Decision Theory: A Brief Introduction*, Royal Institute of Technology, rev. 2005.

Hitchens, Theresa, "DoD Must Brace for Long-Term Supply Chain Problems; Big Mergers Likely," *Breaking Defense*, April 28, 2020.

Janes Intelligence Briefings, "Covid-19: Janes Defense Industry Conversations with Senior DoD Leaders," webpage, 2020. As of August 17, 2023: https://customer.janes.com/Janes/Display/FG_3001982-JIBR

Jones, Marc, "Snarled-Up Ports Point to Worsening Supply Chain Woes—Report," Reuters, May 3, 2022.

Katsaliaki, K., P. Galetsi, and S. Kumar, "Supply Chain Disruptions and Resilience: A Major Review and Future Research Agenda," *Annals of Operations Research*, Vol. 319, *Special Issue: Design and Management of Humanitarian Supply Chains*, 2021.

Leslie, Jacques, "How Climate Change Is Disrupting the Global Supply Chain," *Yale Environment 360*, March 10, 2022.

Lopez, C. Todd, "COVID-19 Response Sparks Efforts to Strengthen Supply Chain," U.S. Department of Defense, September 29, 2020.

Lucas, Rebecca, and Trevor Taylor, "Sealing Technology Transfer Leaks: The Whack-a-Mole Analogy," *RUSI Journal*, Vol. 166, No. 1, 2021.

Luft, Joe, and Harry Ingham, "The Johari Window, a Graphic Model of Interpersonal Awareness," *Proceedings of the Western Training Laboratory in Group Development*, 1955.

Maharjan, Rajali, and Hironori Kato, "Resilient Supply Chain Network Design: A Systematic Literature Review," *Transport Reviews*, Vol. 42, No. 6, 2022.

Maidment, Paul, "Ash in the Supply Chain," *Forbes*, May 17, 2010.

Melnyk, Steven A., Edward W. Davis, Robert E. Spekman, and Joseph Sandor, "Outcome-Driven Supply Chains," *MIT Sloan Management Review*, January 1, 2010.

Mentzer, John T., William DeWitt, James S. Keebler, Soonhong Min, Nancy W. Nix, Carlo D. Smith, and Zach G. Zacharia, "Defining Supply Chain Management," *Journal of Business Logistics*, Vol. 22, No. 2, 2001.

Mian, J., J. Reier Huse, X. Aldea Borruel, and V. Doumeizel, "Resilience and Complex Interdependencies Within and Between Global Food Supply Networks and Transportation Infrastructure," *Cereal Foods World*, Vol. 65, No. 1, 2020.

Muravska, Julia, Anna Knack, Rebecca Lucas, and Ben Williams, *Challenges and Barriers That Limit the Productivity and Competitiveness of UK Defence Supply Chains*, RAND Corporation, PE-A117-1, July 2021. As of January 19, 2024:
https://www.rand.org/pubs/perspectives/PEA117-1.html

Nakano, Mikihisa, and Antonio K. W. Lau, "A Systematic Review on Supply Chain Risk Management: Using the Strategy-Structure-Process-Performance Framework," *International Journal of Logistics Research and Applications*, Vol. 23, No. 5, 2020.

Narasimhan, Ram, Soo Wook Kim, and Keah Choon Tan, "An Empirical Investigation of Supply Chain Strategy Typologies and Relationships to Performance," *International Journal of Production Research*, Vol. 46, No. 18, 2008.

Narayanan, Arunachalam, and Nezih Altay, "Ambidextrous Humanitarian Organizations," *Annals of Operational Research*, 2021.

NATO—*See* North Atlantic Treaty Organization.

North Atlantic Treaty Organization, *NATO Logistics Handbook*, 2012.

Olivares-Aguila, Jessica, and Alejandro Vital-Soto, "Supply Chain Resilience Roadmaps for Major Disruptions," *Logistics*, Vol. 5, No. 4, 2021.

Osinga, Frans, "Organizing for Insecurity and Chaos: Resilience in Modern Military Theory," in Robert Beeres, Gwendolyn Bakx, Erik de Waard, and Sebastiaan Rietjens, eds., *NL ARMS Netherlands Annual Review of Military Studies 2016: Organising for Safety and Security in Military Organizations*, Asser Press, 2016.

Peck, H., "Reconciling Supply Chain Vulnerability, Risk and Supply Chain Management," *International Journal of Logistics: Research and Applications*, Vol. 9, No. 2, 2006.

Perez-Franco, R., S. Phadnis, C. Caplice, and Y. Sheffi, "Rethinking Supply Chain Strategy as a Conceptual System," *International Journal of Production Economics*, Vol. 182, 2016.

Ponis, Stavros, and Epaminondas Koronis, "Supply Chain Resilience: Definition of Concept and Its Formative Elements," *Journal of Applied Business Research*, Vol. 28, No. 5, 2012.

Ponomarov, Serhiy Y., and Mary C. Holcomb, "Understanding the Concept of Supply Chain Resilience," *International Journal of Logistics Management*, Vol. 20, No. 1, 2009.

Proujansky, Adam, "CARES Act: Significant Funds for Defense Department and Defense Contractors," *JD Supra*, April 1, 2020.

Ramirez-Peña, Magdalena, Alejandro J. Sánchez Sotano, Víctor Pérez-Fernandez, Francisco J. Abad, and Moises Batista, "Achieving a Sustainable Shipbuilding Supply Chain Under I4.0 Perspective," *Journal of Cleaner Production*, Vol. 244, 2020.

RAND Europe, "Identifying Conflict-Affected and High-Risk Areas for EU Importers of Minerals," webpage, 2020. As of August 30, 2022: https://www.rand.org/randeurope/research/projects/identifying-conflict-affected-and-high-risk-areas-for-eu-importe.html

Ribeiro, João Pires, and Ana Barbosa-Povoa, "Supply Chain Resilience: Definitions and Quantitative Modelling Approaches—A Literature Review," *Computers & Industrial Engineering*, Vol. 115, January 2018.

Ryczynski, Jacek, and Agnieszka A. Tubis, "Tactical Risk Assessment Method for Resilient Fuel Supply Chains for a Military Peacekeeping Operation," *Energies*, Vol. 14, No. 15, 2021.

Sethi, Sanjay, and Sunil Sharma, "Performance Measurement of Military Supply Chains," *International Journal of Engineering and Management Research*, Vol. 8, No. 2, 2018.

Sheffi, Yossi, and James B. Rice Jr., "A Supply Chain View of the Resilient Enterprise," *MIT Sloan Management Review*, October 15, 2005.

Shih, Willy C., "Global Supply Chains in a Post-Pandemic World," *Harvard Business Review*, September–October 2020.

Singh, Rajesh Kumar, Ayush Gupta, and Angappa Gunasekaran, "Analysing the Interaction of Factors for Resilient Humanitarian Supply Chains," *International Journal of Production Research*, Vol. 56, No. 21, 2018.

Sobb, Theresa May, and Benjamin Turnbull, "Assessment of Cyber Security Implications of New Technology Integrations into Military Supply Chains," *2020 IEEE Security and Privacy Workshops (SPW)*, 2020.

Sokri, Abderrahmane, "Military Supply Chain Flexibility Measures," *Journal of Modelling in Management*, Vol. 9, No. 1, 2014.

Summers, Matthew, "Resilience in Defense Supply Chains," in Jeremy C. D. Smith, ed., *Defence Logistics: Enabling and Sustaining Successful Military Operations*, Kogan Page Limited, 2018.

Taleb, Nassim Nicholas, *The Black Swan: The Impact of the Highly Improbable*, Taylor and Francis, 2017.

Tang, Christopher S., "Robust Strategies for Mitigating Supply Chain Disruptions," *International Journal of Logistics: Research and Applications*, Vol. 9, No. 1, 2006.

Taylor, Trevor, and Rebecca Lucas, "Management of Cyber Security in Defence Supply Chains," *RUSI Journal*, Vol. 40, No. 3, 2020.

Turnbull, Benjamin, "Cyber-Resilient Supply Chains: Mission Assurance in the Future Operating Environment," *Australian Army Journal*, Vol. XIV, No. 3, 2018.

UK MOD—*See* United Kingdom Ministry of Defence.

United Kingdom Ministry of Defence, "Competition Document: Autonomous Last Mile Resupply," webpage, June 29, 2017. As of January 31, 2023: https://www.gov.uk/government/publications/accelerator-competition-autonomous-last-mile-supply/accelerator-competition-autonomous-last-mile-resupply

United Kingdom Ministry of Defence Strategic Command, "Policy Paper: Defence Supply Chain Strategy," webpage, November 15, 2022. As of January 25, 2023: https://www.gov.uk/government/publications/defence-supply-chain-strategy/defence-supply-chain-strategy

U.S. Department of Defense, "DoD News Briefing—Secretary Rumsfeld and Gen. Myers," webpage, 2002. As of June 20, 2022: https://archive.ph/20180320091111/http://archive.defense.gov/Transcripts/Transcript.aspx#selection-401.0-406.0

Van Kampen, Ton, Paul C. Van Fenema, and Nynke Faber, "Strategic Defence Supply Chain Security Management," in Robert Beeres, Gwendolyn Bakx, Erik de Waard, and Sebastiaan Rietjens, eds., *NL ARMS Netherlands Annual Review of Military Studies 2016: Organising for Safety and Security in Military Organizations*, Asser Press, 2016.

Vilko, Jyri, Paavo Ritala, and Jukka Hallikas, "Risk Management Abilities in Multimodal Maritime Supply Chains: Visibility and Control Perspectives," *Accident Analysis & Prevention*, Vol. 123, 2019.

Wirth, Anna Jean, Sydney Litterer, Elvira N. Loredo, Laura H. Baldwin, and Ricardo Sanchez, *Keeping the Defense Industrial Base Afloat During COVID-19: A Review of Department of Defense and Federal Government Policies and Investments in the Defense Industrial Base*, RAND Corporation, RR-A1392-1, 2021. As of January 3, 2024: https://www.rand.org/pubs/research_reports/RRA1392-1.html

Xiong, Biao, Rong Fan, Shuai Wang, Bixin Li, and Can Wang, "Performance Evaluation and Disruption Recovery for Military Supply Chain Network," *Hindawi*, 2020.

Zhao, Kang, Akhil Kumar, Terry P. Harrison, and John Yen, "Analysing the Resilience of Complex Supply Network Topologies Against Random and Targeted Disruptions," *IEEE Systems Journal*, Vol. 5, No. 1, 2011.

The authors' goal was to understand how defense supply chains can better withstand unanticipated and highly impactful disruptions whose probability and impact cannot be readily calculated or quantified. Specifically, the project team set out to identify the current state of the research on supply chain risk management (SCRM), supply chain disruption management (SCDM), and supply chain resilience, both within the defense sector and across the broader commercial landscape. The project team explored the unique characteristics of defense sector supply chains and the ways in which practices from other sectors might or might not be applicable. The team also sought to identify knowledge gaps or broader questions that might not appear in the literature. This study was co-led by RAND and the Swedish Defence Research Agency (Totalförsvarets forskningsinstitut).

The authors found that more research is required to identify good strategies for SCDM for defense, as well as to identify how supply chain specialists and defense and security policymakers might implement these strategies across both the private sector and government. The authors therefore created a research agenda to help fill existing gaps in understanding how defense supply chains can better resist and recover from disruption.

www.rand.org

RR-A2504-1