SUPPLY CHAINS AND SECURITY EXTERNALITIES: AN INTERDISCIPLINARY APPROACH

Occasional Paper No. 2

Dr. William J. Norris and Joseph Balmain Rodgers

The ESP Occasional Papers are a numbered series of policy memos, essays, research papers or reports that contribute to the debate on specific issues relevant to economic statecraft. They may be based on work carried out by researchers granted by ESP, on contributions prepared by external experts, on collective research projects, working groups, or other ESP activities.
Supply Chains and Security Externalities: An Interdisciplinary Approach

Dr. William Norris and Joseph Balmain Rodgers
Texas A&M University

DRAFT Please do not circulate without prior permission from the Authors
Corresponding author: jrogers2177@tamu.edu

Presented at:
The International Studies Association Annual Meeting
Las Vegas, NV (Virtual due to COVID-19)
April, 2021

Abstract

What is supply chain security? How have the US Government and industry approached this set of challenges? Why do supply chain security challenges tend to occur in the first place? How might we think about the relationship between supply chain security and broader security concerns? What can be done about supply chain security? This paper seeks to examine some of the important questions in this emerging topic area and creatively explore possible ways of addressing the complex challenges in this space. Specifically, the paper outlines a creative approach to quantifying (and eventually pricing) supply chain security risk. This paper takes an interdisciplinary approach to supply chain security, focusing on insights from both the business literature and international relations.
Introduction

As the world recovers from the SARS-CoV-2 global pandemic, governments and private businesses have suffered major blows to their supply chains. Multiplying logistical challenges and shortages of raw materials and manufactured goods have forced companies such as Toyota, Samsung, and Honda to halt or reduce manufacturing operations.\footnote{Dan Strumpf and Sean McLain, “Toyota, Honda Shut U.S. Factories as Supplies Run Short,” \textit{Wall Street Journal}, March 17, 2021, https://www.wsj.com/articles/honda-to-close-u-s-factories-for-a-week-over-supply-issues-11615954099.} In addition to such unintentional disruptions that have become daily occurrences, supply chains are threatened by foreign state and non-state actors.\footnote{Susan Lund et al., “Risk, Resilience, and Rebalancing in Global Value Chains | McKinsey” (McKinsey Global Institute, August 2020), https://www.mckinsey.com/business-functions/operations/our-insights/risk-resilience-and-rebalancing-in-global-value-chains#.} Governments acknowledge the national security and economic implications of insecure supply chains and the necessity to shore up potential and existing vulnerabilities.

To better understand supply chain security, we must first answer several basic questions. What is supply chain security? What are the most significant challenges to supply chain security? Why do these challenges occur in the first place, and how have the U.S. government and the private sector approached such challenges? What sorts of frameworks might be most useful for describing the relationship between these challenges and broader security concerns? This paper will begin to answer these questions through four key sections. First, the paper will begin with some of the basic principles of supply chain security. This includes defining the term supply chain security and other key terminology. Second, we describe some of the challenges and threats to supply chain security. Third, the paper will suggest a framework (based on the idea of security externalities) for thinking about how supply chain risks can impact national security. The paper will frame supply chain security within this broader security externality concept to
better understand the various ways supply chains affect national security and military capabilities. Finally, we explore some possible measures to begin to address supply chain security challenges. These include modeling of supply chain vulnerabilities using digital twins and a proposed mechanism for better internalizing and pricing supply chain risk.

Principles of Supply Chain Security

What is supply chain security? Supply chain security strives to prevent the introduction of unauthorized contraband and protect assets from theft, damage, or terrorism.\(^3\) Threats to supply chains include both deliberate efforts to infiltrate and corrupt supply chains as well as accidental events that can disrupt the reliability and predictability of supply. Fundamentally, security is a “sense of insurance against a hazard,” therefore supply chain security seeks to guard against hazards that plague the supply chain.\(^4\) Supply chains are the upstream production relationships and capabilities that provide inputs to a firm's production capabilities. As part of economic specialization and the logic of globalized comparative advantage, supply chains have become disaggregated and frequently distributed across interdependent networks that, today, often span continents. As supply chains have become inherently international over the past century, the number of potential vulnerabilities among the links in a chain has multiplied. For example, one source of supply chain security concern since 9/11 has been terrorist attacks. As supply chains have become digitized, geographically-based risks have also given way to technological ones. The reliance on technology for logistics and operations have made public and

---


private actors vulnerable to cyberattacks, glitches, and other cybersecurity threats related to supply chain security. For example, the cyber domain enables terrorists to no longer be bound by the physical geography in which they are located. Both cyber and physical supply chain security risks have often been borne (de facto) by downstream partners and consumers rather than the producing firm. In other words, costs of such risks often do not map onto the source of the risk. Perhaps unsurprisingly, this creates an absence of incentive for firms to adequately address and plan against risks in supply chains. This has required companies to perform what amounts to herculean due diligence on upstream partners to have confidence in the resiliency of their supply chains.

Notably, supply chain security differs from other terms in the supply chain space. For instance, reliability is defined as “the probability that a product operates properly for a given period of time,” and is rarely used to describe end-to-end supply chains. Instead, we can use the term reliability to describe a specific product or component’s ability to perform in the intended manner and for the expected duration. Reliability is thus a measure of product quality and, while it can be negatively affected by a compromised supply chain, is conceptually distinct from supply chain security itself. Resiliency is defined as “the ability of a system to quickly react to the undesired events when they happen.” Whereas reliability is used to describe a specific output, resiliency is used to describe the robustness of an entire supply chain system. The term resiliency implies that the potential for supply chain disruption is always possible but emphasizes the ability of the supply system to recover and adapt to possible disruptions. While these factors

---

of product-specific reliability and supply chain resiliency should be considered when measuring the integrity or vulnerabilities of supply chains, they slightly differ from supply chain security itself. Supply chain security refers to all of the risks to the integrity of a supply chain. These risks can be accidental or result from the deliberate efforts of a nefarious actor intending to compromise the integrity of a supply chain. The risks can pose threats to the quantity or quality of specific products or outputs of a supply chain (i.e. reliability) as well as threaten the ability of the supply chain system to function properly as a whole (partially captured by resiliency). Whereas supply resiliency emphasizes the ability of a supply chain to recover after having taken a hit, supply chain security focuses more on defending the supply chain from risk factors that could threaten the supply chain in the first place.

All three of these terms (product reliability, supply chain resiliency, and supply chain security) can affect national security which consists of “national defense and the protection of a series of geopolitical, economic, and other interests” in the context of “the safekeeping of [a] nation as a whole.” This definition incorporates the protection of critical supply chains since they affect military readiness and domestic robustness. Vulnerabilities in supply chain resiliency and reliability can have negative effects on national security. Supply chain security tends to emphasize purposeful attempts to disrupt the supply chain and breaches often imply direct consequences for national security. The four major sources of supply chain risk discussed below will build upon the idea of supply chain security and resiliency.

Deliberate efforts on the part of malicious foreign entities to compromise, sabotage or infiltrate supply chains are perhaps the most dangerous source of supply chain security risk and can cause significant harm to a country’s national security. Those supply chain security risks

---

include the insertion of counterfeit goods in defense and dual-use supply chains, foreign
dependency for critical upstream and downstream products and processes, and inadequate
security infrastructure and preparedness on the part of small and medium enterprises (SMEs).
Such inadequacies can be especially troubling especially in those SMEs that service the defense
acquisitions process. Additionally, supply chains incur a risk of disruption or being delayed since
many firms do not carry spare inventory or maintain idle capacity that could help cushion a
failure in upstream supply. Both spare inventory and idle capacity are costly and relatively
inefficient for firms at the microeconomic level. Inventory reduction has progressed gradually
across industries over the last 30 years as part of an effort to reduce costs by lowering operating
capital requirements. Getting comfortable with taking on such risks from just-in-time sourcing
required advances in supply chain risk management which is “the identification and management
of risks for the supply chain, through a coordinated approach amongst supply chain members, to
reduce vulnerability as a whole.” As can sometimes be the case, such risk management
occasionally systematically overlooks or underweights entire categories of risk. Such
misattributions may go undetected for years until a shock or unusual event calls attention to an
industry’s exposure.

The U.S. government and partner industry players have occasionally taken measures such
as stockpiling supplies of critical materials, developing a base of trusted suppliers, and building
redundancies into the supply chain. All of these measures are designed to hedge against supply
chain risks. Yet, all of these measures “are imperfect, potentially quite costly, and relatively
inefficient.” In order to develop a better solution that addresses the core challenges for supply

---

8 Closs and McGarrell, “Enhancing Security Throughout the Supply Chain.”
9 Norris, William, Joseph Balmain Rodgers, Chase Blazek, Tarni Hewage, and Braeden Kobza. "A Market-Oriented
chain security, we now turn to take a closer look at the various types of threats facing supply chains.

Types of Supply Chain Security Challenges

Although the possible challenges posed to supply chains are myriad, this paper identifies four major sources of supply chain threats that can most directly affect national security: counterfeit goods (which impact reliability), foreign dependency, insufficient security infrastructure within a supply chain, and lack of contingency capacity. While there may be additional national security-related supply chain challenges that do not fall into one of these types, we find these threats to be among the most commonly addressed in the supply chain literature. Each of these loom large when evaluating supply chain security and resiliency. This section provides additional details on these four types of risk and their links to national security.

Counterfeit goods can adversely affect product and process reliability as well as compromise product integrity when introduced into supply chains that are critical to national security and economic operations. This is a vulnerability that directly affects military performance as recognized by a Government Accountability Office (GAO) report: “[Counterfeit goods] have the potential to seriously disrupt the DoD supply chain, delay missions, and affect

---

the integrity of weapon systems.”¹¹ Even if these parts do not affect military efficacy, they impose excessive economic burdens on government agencies and firms alike. The Senate Armed Services Committee released a 2012 report that detailed a case in which counterfeit goods forced the Missile Defense Agency and its contractors to invest $4.5 million in reworking costs.¹² The same report discovered that 70 percent of the 100 counterfeit parts that the committee traced were manufactured in China. Although counterfeit goods can be deceptive or non-deceptive in nature, the capability for disruption remains the same and, according to the Senate Armed Services Committee, the Chinese government has failed to combat the open manufacturing of counterfeit goods in its domestic market. Whether China deceptively and deliberately injects counterfeits into a supply chain or simply fails to crack down on the production of counterfeit goods (thus increasing the likelihood of introducing compromised parts), the detrimental effects can be costly. Actions as well as inactions can have a negative influence on the U.S. economy and national security.

A second source of threat to supply chains is concentrated dependency. Reliance on a single source for an input or raw material exposes a supply chain to vulnerability. Such placing of all of one’s eggs in a single basket can risk supply chain failure if something happens to that unique source of critical supply. When such upstream supply dependency rests on foreign suppliers or firms, the dependency can be leveraged for international advantage since such dependency exposes companies and governments to increased international political and economic risks. Such sources of supply are also subject to another nation’s domestic political

economic institutional factors that can facilitate manipulation of access to this critical source. Globalization has allowed supply chains to leverage the economic benefits of comparative advantage by manufacturing and procuring certain goods and materials from the most inexpensive source. However, the outcome of this micro-economically rational cost saving set of decisions often results in routing some supply chains through a single nation without any close replacements or redundancies. Such unique dependence can expose firms to unexpected risk. For instance, the SARS-CoV-2 pandemic revealed the risk of supply shocks when the Indian government enacted export controls on 26 active pharmaceutical ingredients (APIs). Overreliance on India for these products forced downstream importers to scramble to find substitutes or reduce or halt production of pharmaceuticals. In this case, Europe faced the prospect of a shortage of pharmaceuticals which harmed public health. This is far from the only case of foreign dependency. The U.S. is completely reliant on the imports of 19 minerals used in the production of defense systems, high tech, and clean energy industries. 17 of these minerals are sourced from China which developed a major commercial advantage in the mining and processing of such minerals through predatory business tactics and lenient regulations. A major source of the U.S. government’s supply chain security concerns revolve around China purposefully withholding critical materials and products from American companies. Threats from Beijing to create a rare earths “blacklist” of companies that are perceived to harm Chinese

---

13 This behavior has often over-weighted the attractive economic benefits while under-weighting the supply chain risk.
interests fuel U.S. concerns about supply chains and dependency on foreign competitors for many materials. While political or diplomatic friction can drive such suspensions, a simple natural disaster supply shock or increased domestic demand can produce a similarly disruptive shortage. Such disruptions can occur whether the producing nation is a U.S. ally, adversary, or acting with deliberate malicious intent. Whether China purposefully uses raw material dependency as a geopolitical bargaining chip or if a supply shock is the product of weather, the effect on American defense companies and the military could be equally debilitating. They would be deprived of their ability to manufacture and procure systems integral to national security.

The third type of supply chain vulnerability that often affects national security is inadequate security infrastructure; including, but not limited to, information technology systems. Globalization has fundamentally changed the dynamics of supply chain vulnerability. Given levels of inter- and intra-enterprise systems integration, the security integrity of a globalized supply chain is only as strong as its weakest link. In other words, suppliers, distributors, and even consumers that lack adequate security measures possess the potential to corrupt the entire supply chain. Department of Defense (DoD) officials and reports have confirmed that SMEs often lack adequate security infrastructure. Such vulnerabilities in supply chain partners can expose an entire program to unacceptable levels of risk. Under Secretary of Defense for Acquisition and Sustainment Ellen Lord testified to the Senate Armed Services Committee in October 2020 that

---

24.2% of the entire defense budget was explicitly directed toward small businesses in 2019.\textsuperscript{19} Additionally, subcontract funding for the same fiscal year was $62.3 billion indicating that there is “significant flow down from major defense primes to small businesses.”\textsuperscript{20} Many such small defense firms lack the large amounts of capital required to cover the high fixed costs of enterprise security infrastructure, and are reluctant to raise additional capital through debt or equity beyond what is necessary for business operations and production. Since cash flows are often retained and reinvested to accelerate growth, economic efficiency is prioritized above security which can cause smaller defense firms to be a major liability in the supply chain. This vulnerability is especially salient in manufacturing for two reasons. First, 99% of the 347,000 manufacturers in the U.S. are SMEs, and 50% of SMEs lack basic cyber controls.\textsuperscript{21} Since these firms operate on a small scale, they are often “unaware of federal requirements and may lack the financial and technical capabilities required to manage cybersecurity risks.” Second, manufacturers “received the greatest volume of targeted cyber-attacks of all industries globally” in 2014.\textsuperscript{22} This combination of vulnerability and ubiquity in defense supply chains illustrates the need to bolster the security of SMEs, especially manufacturers that can serve as a link in the supply chains of major defense primes.

Fourth, “just-in-time” sourcing models that have done so much to lower operating capital requirements by reducing inventory stock held on hand, also come with supply chain risk. Firms

\textsuperscript{22} Ibid.
ought to remain wary of business practices that reduce stockpiles and redundancies throughout the supply chain. Such “on-time” sourcing may lower costs, but downstream components, firms, and consumers suffer in the event of a disruption. Without the cushion of some supply on hand, such supply chains precariously rely on other supply chains to reliably deliver replenishment. If supply chains in such a lattice get delayed or disrupted, it can have a cascading downstream network effects all the way to the consumer. A 1997 empirical study of just-in-time (JIT) logistics in global sourcing acknowledged that “JIT supplied companies reported much lower on-hand inventories . . .”\(^\text{23}\) Strategies such as intermediate stocking points often reduce the need for safety-stock, but such strategies and the efficacy of an integrated JIT/global sourcing system depend on the firm’s ability to “effectively manage the longer inventory supply line while reducing lead times and enhancing flexibility.”\(^\text{24}\) Disruptions in the supply chain reduce this efficacy and render strategies such as intermediate stocking points mostly useless–especially if the disruption occurs further upstream in the supply chain. Therefore, despite financial benefits, JIT sourcing models incur the risk of a domino effect down the supply chain. JIT is but one example of a broader failure to ensure adequate contingency capacity for supply chain disruptions. One of the main reasons such risks are tolerated is that the burden of paying the costs when risks and vulnerabilities in a supply chain turn into actualized disruptions and compromises are largely borne by downstream firms and consumers rather than the firms originally responsible for the breach or disruption. Inadequate contingency capacity in supply chains affect resiliency, economic activity, and sometimes national security.


A Security Externality Framework

So when do supply chain risks matter for national security? How might we think about the relationship between supply chain security and broader security concerns? We suggest that a helpful way to frame the relationship between the economic activities of firms (and their supply chain challenges) and the broader arena of states (and the realm of national security) is through the lens of security externalities.

To begin, commercial actors, not states, conduct most of the interactions in international economics. Such interactions are generally driven by profit considerations and mostly produce economic effects that accrue to the transacting parties. But in certain industries or under certain conditions, the activities of firms may also generate security externalities, or security consequences for states. These security externalities are exogenous to the private sector transacting parties who are directly engaging in the economic activity. Nevertheless, a commercially-driven decision, say to sell a business unit to a foreign investor, may result in the transfer of proprietary dual-use chemical manufacturing processes to a rival state. Such security consequences of economic activity are called security externalities.

It would be helpful to be able to map the various ways that the economic activities of firms (e.g. selection of trading partners, investment location decisions, acquisitions, etc.) could tie back to national security concerns of states. We elaborate on just such a framework elsewhere. In this paper, it is sufficient to briefly introduce the typology and explain the six

---


different causal logics that can link the economic activities of firms to the national security of a state. Then, we can contextualize supply chain security concerns using this framework.

Primarily, there are two pathways by which economic interactions can impact a nation’s security: a Military Channel and an Economic Channel. Economic activity can carry direct military effects or can impact a nation’s security by acting primarily through economic channels. The six different types of security externalities discussed below map onto these two broad families.

The externalities in the Military Channel share the common causal logic that a nation’s war-fighting capacity can be directly strengthened or weakened by economic activity. For example, one can envision a compromised supply chain in the defense procurement arena hampering the military effectiveness of a new weapons system. This would have a “disarming” effect on a nation’s security. Likewise, technology transfer that might accrue to a host nation as a result of a portion of an intercontinental supply chain in a dual-use industry being outsourced and now resident in that host nation would have the opposite effect on that host nation. Such a
security externality might usefully be characterized as “arming” or largely beneficial to the host nation’s national security.

Similarly, strengthening or weakening a target nation’s economy as a whole can carry implications for the long run capabilities of a state. This is based on the principle that economic power is the foundation of national security over the medium and long run. For instance, senior leaders in the U.S. Army and Navy recognized the necessity to maintain a robust and technologically progressive domestic aircraft industry as well as foster commercial aviation during and after World War I. Although the use of aircraft at the time was limited, this assumption proved true when technical developments in European and American aviation played a major airpower role during World War II. By extension, firm activities that enhance the vitality of a nation’s economy may be characterized as strengthening that nation’s security, while activities that erode competitiveness or innovation capacity can be accurately described as detrimental. These types of security effects reside in the Economic Channel which is the other main branch of the typology. For this family of externalities, security ramifications are second-order derivatives of the economic interaction as opposed to the military effects branch of the typology in which economic interaction directly contributes or detracts from a state’s ability to wage war.

---

27 A prime example of economic power serving as a foundation for national security is the history of the British Royal Navy. Britain’s declining economy after World War I catalyzed a drastic reduction in the production of naval vessels, delaying the Royal Navy’s armament plans. Consequently, the British capacity to project security across its colonial holdings was gravely threatened, especially its imperial holdings in Asia. By the onset of World War II, Britain could not afford to deploy the Royal Navy across the globe due to maritime security threats from the Axis Powers, chiefly Germany. Additionally, they lacked the human, physical, and intellectual capital to construct new vessels at a rate that would surpass the United States or Japan whose shipbuilding industries were robust. Through this case study, Paul Kennedy explicitly links the commercial shipbuilding industry within Britain as foundational to London’s construction of a world-class navy. For more information on how the shipbuilding industry affected Britain’s military capabilities, see Paul Kennedy, *The Rise and Fall of British Naval Mastery* (Penguin UK, 2017).

The economic branch is subdivided into two groups: those types of externalities that affect the overall health of the target economy as an end in itself (discussed in the preceding paragraph), and those security externalities in which the economic interaction plays an instrumental rather than teleological role. In the “Economy as a Means” group, two distinct strategic logics connect the economic activity back to security. The first is a transactional logic that seeks some contingent outcome in exchange for market access, cessation of sanctions, freezing bank accounts, or other kinds of actions that seek to alter the target’s behavior. The second is a deeper transformational logic in which the economic activity shapes and redefines how the target state views its own best interests.

These six types of security externalities—arming (strengthening target’s military capability), disarming (weakening target’s military capability), corrosion (weakening target’s economy), bolstering (strengthening target’s economy), transactional, and transformational—all illustrate the relationship between the economic activity of firms and the resulting effect on a nation’s broader national security. Elsewhere, we have laid out a fuller theoretical treatment of this approach to economic statecraft, but for our purposes here, it suffices to show how the supply chain decisions of firms can involve ramifications for security—particularly when those supply chains fall victim to some of the types of threats laid out in the section above.

This security externality framework can provide a clearer vocabulary and explicit causal logics that link the activities of firms back to the security of states. Such a framework can be useful for delineating exactly how a particular supply chain vulnerability may impact national security. For example, asymmetric dependency for a critical material in supply chains may be leveraged by a nation holding the stocks. In other words, a transactional type of security externality can be said to rest primarily on dependence. Such single points of failure in a supply
chain were highlighted above as being a source of vulnerability. This dependence can be on a monopoly or a monopsony, or dependence on a single entity for supply or demand, respectively. The more inelastic or asymmetrical the dependence is, the easier it will be to harness that dependence for coercive purposes.

Beyond dependence, the other supply chain security risks can also be understood using this security externalities framework. For example, counterfeits in the military procurement (defense-related equipment and materials) supply chain negatively affect war-waging capabilities. This is an example of supply chain security risks that operate along a disarming type of security externalities logic. Such infiltration of supply chains incurs large economic costs and possible threats to national security, as indicated earlier. To the extent that counterfeits undermine intellectual property, fail to perform reliably, or erode a nation’s innovation enterprise, they can also be said to be operating against the health of the economy, more generally.

Additionally, the security externalities framework enables analysts to specify the causal logic that connects insufficient security infrastructure inherent in many SMEs back to national security concerns. The security externalities approach can help distinguish among the distinct ways such vulnerabilities can result in national security effects. For example, a disarming logic resulting from malicious code in a defense supply chain component operates in a different way than the transactional logic of ransomware, even though both may be types of security externalities that could be exploited as a result of an SME’s breached server. Similarly, this framework helps think through the pathways by which a lack of supply chain redundancies might affect national security. In short, this typology allows for more accurate analysis and modeling of
supply chains, and, consequently, more effective solutions to predict, prevent, and mitigate supply chain security and resiliency risks.

What Can Be Done About Supply Chain Security?

The answer to this question lies in the more fundamental question of why do vulnerabilities in the supply chain persist and arise in the first place? We find that supply chain security risks tend to come about (and persist) primarily for two reasons.

First, the complex structure of modern manufacturing supply chains makes it difficult or nearly impossible for end users to detect and identify compromised links. Over the past few decades, U.S. manufacturers have embraced a “multi-tiered” structure of interdependencies where more specialized parts and components are outsourced to first-tier suppliers which may subsequently outsource more specialized components to second-tier and below suppliers. To illustrate, Airbus has 1,676 publicly disclosed “tier one” suppliers, but has over 12,000 “tier two and below” suppliers. General Motors has 856 and over 18,000 of each, respectively. Second-tier suppliers may outsource further to a third or fourth-tier which become increasingly smaller in scale, more specialized, and less visible to the prime firm and central supply chain. In fact, such “fourth-tier” suppliers may participate in the supply chain unbeknownst to the primary firm. When such a firm is a major defense prime contractor such issues of transparency can become threats to national security. Transparency, or visibility as McKinsey refers to it, represents “the extent to which [a] customer can trace spending at [a] subtier level.” As more subtiers are introduced to a supply chain, it becomes more complex and difficult to locate vulnerabilities and mitigate security breaches. Resulting damage experienced through breaches in “fourth-tier”

30 Ibid.
suppliers could hold the main defense prime liable for unlawful or unethical activity leading to expensive lawsuits. Additionally, vulnerable downstream or upstream partners could expose the main firm to intellectual property theft, exploited information security vulnerabilities, and operational delays. Addressing such violations after occurrence can lead to compromised brand integrity and considerable losses of time and money. This diminishes supply chain resiliency which can have a negative effect on supply chain and national security. This problem of opacity, combined with insufficient security measures common in “fourth-tier” suppliers, becomes a major source of risk in the supply chain that carries great potential for widespread disruption.

Second, supply chain security risks often are not fully internalized by the responsible firm. As a result, it is rational for parties in the supply chain to shirk costs associated with mitigating supply chain vulnerabilities. Most of the burden for supply chain disruptions (delays, stock-outs, faulty products, etc.) tend to be borne by downstream partners rather than the producing firms that could have been in a position to take steps to limit disruption and ensure the resiliency and security of their supply chains. Downstream partners can be intermediate customers who rely on semi-finished goods or products or services from the compromised supply chain. They can also be end user customers who are forced to forgo access to the good or to seek an alternative source of supply when original supply chains fail to deliver.

To address the challenge of complexity and the ensuing challenges of visibility, we suggest the use of agent-based modelling and digital twins. These are complex models that are designed to accurately reflect the complexity of a supply chain for a particular firm. Such digital twins could then be used to simulate potential supply chain disruptions. This enables a firm or an industry to better appreciate and anticipate possible supply chain disruptions before they actually occur. Historically, firms have relied on large volumes of periodically-updated data to identify
and respond to supply chain vulnerabilities and risks. Thus, adjustments made to the supply chain were reactive (rather than proactive) and insufficient to mitigate risks that are increasingly dynamic in nature. Digital twins collect real-time streams of fine-grained data which allows for advanced, prescriptive supply chain modeling and analysis. Inputs are fed into the simulation in real time, and the simulation considers more categories of data other than exclusively historical cases. Through these game-changing advantages, digital twins promise firms complete end-to-end visibility of their supply chains to improve resiliency, security, and test contingency planning. This is especially valuable for supply chains with multiple tiers; digital twins provide transparency and visibility where there was little to none before.

This modeling approach leverages several of the cutting-edge trends in industrial supply chains. The structure of a digital twin allows it to model product development and general status of parts and tools in asset-intensive industries. These models are composed of three major capabilities: robust analysis (decision-support) capabilities built around simulations, big data science, and optimization; information modeling and data curation; and data connectivity and collection enabling dynamic representation and synchronization of digital models. Thus, digital twins utilize key capabilities that are redefining traditional manufacturing through automation as part of Industry 4.0. This includes large-scale machine-to-machine (M2M) communication powered by the Internet of Things (IoT), big data analytics, and artificial intelligence which boosts simulation and detection capabilities. Such simulations, however, require the construction of the model which is initially intensive, tedious, and time-consuming. Software engineers and others must gather all required data from disparate sources and ensure it is accurate and updated. Additionally, the software architecture to host and serve as a platform to run the simulations must be developed. More open-source data on abstraction frameworks or model libraries would
allow for swifter development of these simulations, but this is currently a major gap in the mainstream software engineering research community. Through Industry 4.0 and the rise and adoption of associated technologies, digital twins hold out the promise of greater visibility into supply chains. They can be a solution for capturing the complexity of contemporary supply chains and can help mitigate against some supply chain security risk by predicting and detecting potential vulnerabilities.

In addition to digital twins, we have also proposed an idea to help internalize some of the largely externally-borne costs that result from supply chain risk. This concept of a supply chain risk assessing system (RAS) was published in the journal *Security Challenges*, and mainly discussed supply chain security for the defense acquisitions industry. Specifically, we proposed the groundwork for a potential solution that quantified individual firms’ supply chain security risks modelled after the FICO credit score system used in the U.S. Similarly to how the FICO score is structured through five predetermined weighted factors, the RAS score would be calculated based on empirical correlates from actual incidents. The exact calculations and scoring would be determined by competing risk assessment agencies that would develop algorithms to process proprietary datasets to assess supply chain security risks and forecast damages. Over time, these algorithms would increase in accuracy and more precisely be able to quantify (and eventually, price) risk. The resulting score could be publicly available to investors, the Department of Defense, and other relevant stakeholders that value firms with robust supply chain security and resiliency. By making the RAS scores public, firms would be incentivized by competitive market dynamics (such as successfully bidding for contracts and competitive brand advantages stemming from better scores) to invest in supply chain security measures and perform due diligence on upstream suppliers. Both of these countermeasures to supply chain
security risks tend to be under-provided by the market today because they are costly with little quantifiable returns to justify the outlays. The supply chain security risk assessing system (RAS) helps to address these challenges.

In sum, supply chain vulnerabilities persist for two reasons. First, firms and governments are unaware of such risks due to lack of visibility into highly complex, multi-tiered supply chains. Second, the costs from supply chain disruptions are largely borne by downstream partners. Those nodes of the supply chain that would be best placed to take measures to mitigate risks do not bear most of the costs when supply chains fail and thus have little to no incentive to expend costly effort to address them. When such consequences are externalized, it is not a mystery why market solutions under-provide supply chain risk mitigation.

Digital twins and the supply chain security risk assessing system (RAS) resolve both structural challenges by granting firms the ability and motivation to detect and resolve supply chain risks. The end-to-end simulative capabilities of digital twins reduce the opaqueness of multi-tiered supply chains while incorporating real-time data. In turn, this data can enhance the algorithms that price and quantify supply chain risks, thus making estimates for financial burdens more accurate and relevant to the parties involved. Since these RAS scores will be public, all firms in the same supply chain are affected financially even if only one component harbors vulnerabilities. RAS will help internalize some of these costs that have historically (often implicitly) been passed on to downstream partners. Both measures will empower supply chains to assume proactive rather than reactive approaches to supply chain security.
Conclusion

Supply chain security, supply chain resiliency, and product reliability have captured the spotlight due to the SARS-CoV-2 pandemic. Supply chain security involves the risks threatening the integrity of the supply chain while resilience focuses on the supply chain’s ability to respond to unforeseen events once they occur. Reliability, however, most commonly describes a specific product’s ability to function properly over time. All three are affected by supply chain challenges. Counterfeit goods, foreign dependency, insufficient security infrastructure, and lack of contingency capacity all play a major role both in empirical reality and in the literature surrounding supply chains. Understanding these risks is crucial to firms and governments’ ability to identify and offset vulnerabilities and threats to the supply chain. Supply chain risks can also affect national security. Our framework of security externalities highlights the manner in which such risks can have distinct effects on national security and a nation’s economy. Mitigating against such risks is of the utmost importance to avoid a position of fragility in either the security or economic domain. Digital twins have the potential to illuminate supply chains on an end-to-end spectrum which would fundamentally shift the paradigm of transparency in supply chains. Rather than inadvertently hosting opaque activity, supply chains would be able to be monitored, even down to the sub-tier levels. In conjunction with digital twins, our proposition of a supply chain security risk assessing system would capitalize on this transparency by assisting firms in predicting and quantifying such risks. By doing so, firms and governments can become aware of what risks will have the largest impact, and therefore they may take measures to counter potential vulnerabilities. With the Risk Assessment System (RAS), the costs of such measures can be offset with quantifiable value reflected in a firm’s RAS score. Higher RAS scores would
support brand integrity and allow for access to certain classes of partnership. These opportunities would be otherwise closed or unavailable to firms with lower scores.

While we make specific recommendations to reduce the opaqueness and risk of supply chains, we acknowledge that there is much more work to be done. First, more research must be done on specific risks supply chains face, especially risks that involve states or state-owned enterprises (SOEs). Current financial regulations in the U.S. requires only scant reporting from private companies, and SEC filings and other documents from public firms often lack specific information concerning supply chains. More must be done to acquire much-needed data about supply chain risks without placing an excessive burden on firms or governments. Second, research and technological capabilities enabling digital twins must be developed. Current efforts to develop real-time simulations of processes (such as supply chains and development of specific products) are time-consuming and tedious. More research is needed in open-source data libraries that will be used to expedite the creation and development of digital twins. Lastly, the prototype to quantify supply chain security risks, RAS, needs to be tested before being scaled up. Since we deliberately do not specify which type of entity should perform risk assessments of private firms’ supply chains, this prototyping should be done in the public and private sectors alike. Private actors would rely on market dynamics to develop pricing algorithms, but this is still likely to require a role for some government oversight (and perhaps warrant the creation of new public entities). Under conditions of uncertainty, this portfolio approach is the best way to allow market forces and results-oriented performance to determine the eventual contours of the RAS system. Both RAS and digital twins should go a long way toward assisting firms combat supply chain security threats that would otherwise jeopardize their operations.