A Market-Oriented Approach to Supply Chain Security

Dr. William Norris, Joseph Balmain Rodgers, Chase Blazek, Tarni Hewage, and Braeden Kobza

Abstract

What is supply chain security and how does it impact national security? Why do certain challenges arise in supply chain security and how can the U.S. Government, its allies, and private industry address these challenges? This article seeks to examine this emerging topic and outline a creative approach to quantifying (and eventually pricing) supply chain security risk. In this piece we argue that firms ought to secure their supply chains and effectively mitigate uncertainties since these risks can disrupt business operations if neglected. Furthermore, these risks also entail national security concerns in the defence acquisitions supply chain. We introduce a novel supply chain risk assessing system that is modelled after the FICO credit scoring system used to measure consumer credit risk.

Introduction

As natural and man-made threats push supply chains to the forefront of global attention, supply chain security seems more relevant than ever. What exactly is supply chain security and how does it impact national security? Supply chain security strives to prevent the introduction of unauthorised contraband and protect assets from theft, damage, or terrorism.[1] Fundamentally, security is a "sense of insurance against a hazard," so supply chain security would guard against hazards that plague the supply chain.[2] However, prioritising supply chain security has been challenging in a globalised world since the economics of comparative advantage, digitalisation, and specialisation have led to disaggregation and distribution choices that, over time, have made supply chains inherently international. This has lengthened supply chains and increased the number of potential vulnerabilities. Additionally, the 9/11 terror attacks expanded the scope of supply chain security beyond combating contraband and theft.[3] By threatening supply chains vital to the Department of Defense (DoD) supply chain security also began to encompass threats to national and economic security. National security is "the safekeeping of [a]

1 David Closs and Edmund McGarrell, "Enhancing Security Throughout the Supply Chain," Special Report Series (IBM Center for The Business of Government, April 2004), http://www.businessofgovernment.org/sites/default/files/Enhancing%20Security.pdf.

2 Zachary Williams, Jason E. Lueg, and Stephen A. LeMay, "Supply Chain Security: An Overview and Research Agenda," ed. Matthew Waller, *The International Journal of Logistics Management* 19, no. 2 (August 15, 2008): 254–81, https://doi.org/10.1108/09574090810895988.

3 Hau L. Lee and Seungjin Whang, "Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management," *International Journal of Production Economics* 96, no. 3 (June 2005): 289–300, https://doi.org/10.1016/j.ijpe.2003.06.003.

nation as a whole," and consists of "national defence and the protection of a series of geopolitical, economic, and other interests."[4] Protecting supply chains, especially those of the defence acquisitions industry, has become a national security concern. If these supply chains are compromised, then the defence-industrial base and the efficacy of defence systems would falter, thus jeopardising national security and allowing foreign adversaries to exploit these deficiencies.

Of course, there are a range of ways one might think of mitigating this sort of risk. Stockpiling supply to cushion the impact of shortages or mandating redundancies in a supply chain would both lower risk but at the expense of considerable inefficiencies and idle inventory. One could also diversify the supplier base or build trusted networks of possible suppliers but in many areas of the defence procurement system, there may only be one or two possible suppliers of a highly specialised component.[5] All of these measures are imperfect, potentially quite costly, and relatively inefficient. In this article, we suggest an alternative, market-based mechanism that seeks to accurately price in security risk and internalise what have typically been externalised costs associated with supply chain security risk. This solution addresses a market failure in the current system: a significant portion of supply chain security risk has historically been borne (*de facto*) by the downstream partners and consumers--not the producing firm. Direct costs are not often co-located with the source of the supply chain risk, namely as part of the cost-benefit calculus of the firm supplying the goods. Traditionally, defence acquisition firms have prioritised cost, scheduling, and performance, and often overlooked security as a result. Neglecting such security risks impacts national security and the long-term vitality of the U.S. defence-industrial base.

Effectively managing supply chain security risk is not limited to the U.S. Other nations such as Vietnam and Japan have experienced supply chain disruptions stemming from concentrated dependence on China. For example, a diplomatic dust-up between Japan and China in 2010 led to a *de facto* ban on rare earth metal exports to Japan.[6] China is responsible for the mining and processing of 95% of the world's rare earth minerals, giving it considerable leverage.[7] The move prompted "...particular alarm in Japan, which

4 Kim Holmes, "What Is National Security?," The Heritage Foundation, October 7, 2014, https://www.heritage.org/military-strength-topical-essays/2015-essays/what-national-security.

5 A report from the Senate Armed Services Committee in 2012 acknowledged that weapon systems used by the military may "depend on the performance and reliability of small, incredibly sophisticated electronic components." "Inquiry Into Counterfeit Electronic Parts In The Department of Defense Supply Chain" (Committee on Armed Services United States Senate, May 21, 2012), https://www.congress.gov/112/crpt/srpt167/CRPT-112srpt167.pdf.

6 In this particular example, the majority of the Western media, including *The New York Times*, characterised China's export ban as a *de jure* embargo since it followed Japan's detention of a Chinese trawler captain. However, the Chinese government denied this accusation and claimed the backlogging of pre-shipment checks had resulted in a *de facto* ban. Despite this discrepancy, China failed to relieve Japan's perception that this was retaliation from Beijing thus raising tensions between two of the largest trading partners in East Asia. Nonetheless, Japan experienced the vulnerability of not receiving critical rare earth metals. Such foreign dependency, regardless of its cause, is a supply chain security risk that threatened Japan's short-term economic vitality.

7 Due to Beijing's lax environmental regulations and the ample supply for cheap labor, many firms in the mining and mineral processing industries sought refuge in China. In other words, China's firm hold on the global market for rare earth metals was not created entirely by intentional design, but was instead based on commercial dynamics and individual, firm-level optimisation. See Valentina Ruiz Leotaud, "Rare Earths: Battling China's Monopoly after Molycorp's Demise?," *Mining.Com*, September 10, 2016, https://www.mining.com/rare-earths-battling-chinas-monopoly-after-molycorps-debacle/.

has few natural resources and has long worried about its dependence on imports."[8] The trade dispute caused Japanese Trade Minister Akihiro Ohata to acknowledge that Japan had not "put enough effort into risk management."[9] This case illustrates that Beijing has the capability—and the will—to weaponise foreign dependencies to achieve its goals. Without rare earth minerals, Japan cannot manufacture products integral to its economy and national security such as hybrid cars and guided missiles.

Japan is not alone in its dependence on Chinese sources of supply. Foreign dependencies like this "[constitute] an unusual and extraordinary threat, which has its source in substantial part outside the United States, to the national security, foreign policy, and economy."[10] Vietnam's trade deficit with China increased by 40% in 2019. Vietnamese electronics manufacturers are dependent on plastics, metals, and other components from China. Countries in Southeast Asia remain "highly dependent on China for equipment and raw materials to power [their] manufacturing sectors."[11] Australia has faced a structurally similar concentration risk, but from the demand (rather than supply) side. China is an important consumer of Australian raw material exports. Such concentrated demand has been a structurally similar source of concern for Australian producers. If Chinese demand slows, this concentrated reliance on a single market drags down both prices and quantities of Australian exports. Supply chain security is a common challenge facing many nations at the outset of the 21st century. Although primarily focused on the empirical context of the US, the supply chain security issues (and potential solutions) raised by this article have broad applicability well-beyond US borders. The security of international supply chains is likely to carry important ramifications (especially for partners and US allies).

To help improve risk management, this article proposes a solution similar to the FICO credit score system which measures consumer credit risk.[12] Such a system could serve as a market-oriented innovation to help identify vulnerabilities in supply chains.[13] In this novel risk assessing system, several different ratings agencies would develop algorithms to assign scores to companies based on known risk factors. Over time, these algorithms would improve as more and more cases of supply chain risk are detected. Eventually, such scores would help to proactively predict what parts of a supply chain are most at risk (much like how a lower credit score helps to distinguish riskier mortgage applicants). These scores will also incentivise firms to minimise the vulnerabilities of their supply

8 Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan—The New York Times," *The New York Times*, September 22, 2010, https://www.nytimes.com/2010/09/23/business/global/23rare.html.

9 Yuko Inoue, "China Lifts Rare Earth Export Ban to Japan: Trader," *Reuters*, September 29, 2010, https://www.reuters.com/article/us-japan-china-export-idUSTRE68S0BT20100929.

10 Joe Gould and Aaron Mehta, "Trump Executive Order Targets Rare Earths Minerals and China," *DefenseNews*, October 1, 2020, https://www.defensenews.com/congress/2020/10/01/trump-executive-order-on-rare-earths-puts-material-risk-in-spotlight/?utm_source=clavis.

11 Manisha Mirchandani, "Coronavirus Exposes Dependency of Southeast Asia's Manufacturers on China," *BRINK—News and Insights on Global Risk*, March 15, 2020, https://www.brinknews.com/coronavirus-exposes-dependency-of-southeast-asias-manufacturers-on-china/.

12 The FICO score was created by the Fair Isaac Corporation for which the score was named. The score was founded in 1958 to empower firms to make better business decisions and expand the availability of credit. A score is assigned by credit scoring agencies to individuals and businesses to be used in lending and other financial decisions. For more information on the FICO credit score, see Shweta Arya, Catherine Eckel, and Colin Wichman, "Anatomy of the Credit Score," *Journal of Economic Behavior & Organization* 95 (November 2013): 175–85, https://doi.org/10.1016/j.jebo.2011.05.005.

13 The origins of this idea stem from conversations Norris had while serving as a fellow with the National Bureau of Asian Research.

chains by making supply chain risk information available to stakeholders in much the same way that personal credit scores are used. Such transparency would empower the DoD, customers, and other stakeholders to hold companies accountable for their potential to introduce risk into a given supply chain. Accountability is crucial in the DoD supply chain since risks, such as that posed by defective counterfeit parts, can threaten national security by compromising critical military operations.[14] In essence, this system would help to "price" supply chain risk and give companies a strong incentive to conduct due diligence when establishing and maintaining their supply chains partners. Under such a system, firms will gravitate toward measures that reduce their supply chain risk exposure, such as diversifying their supplier base to reduce dependency on a single foreign entity. The net result will be more secure supply chains supporting defence needs. Securing vulnerable supply chains is the central goal of this system.

Our framework for exploring this innovative concept will be presented in three sections. First, we explain and identify the unparalleled challenges surrounding supply chains in the twenty-first century. Every industry encounters supply chain challenges, but the defence acquisitions industry is uniquely tied to national security concerns and thus faces an acute need to address supply chain challenges such as counterfeit goods, foreign dependency, and small businesses possessing insufficient security processes. Supply chain security risks like these in the defence acquisitions space directly impact national security. In the second section, we introduce a novel supply chain risk assessing system that is modelled after the FICO credit scoring system used in the U.S. to measure consumer credit risk. The section examines how such a system would work and its unique advantages. Finally, we consider the challenges and limitations of such a supply chain risk assessment system before concluding.

Motivation

The Burgeoning Burden of Supply Chain Security Risks

Understanding the unprecedented difficulties that supply chains face is critical to recognising the consequences of supply chain security and the necessity of a risk assessing system. Defence acquisition firms have a responsibility to perform due diligence when managing their supply chains since their operations are vital to national security. Before describing the various risks that exist in this space, it is appropriate to define some of the terms used throughout the paper. As mentioned earlier, *supply chain security* is "the application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism and to prevent the introduction of unauthorised contraband, people, or weapons of mass destruction into the supply chain."[15] *Supply chain risk management* 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." This paper will not use the explicit term supply chain risk management, but will instead

14 Brandon A. Sullivan and Jeremy M. Wilson, "An Empirical Examination of Product Counterfeiting Crime Impacting the U.S. Military," *Trends in Organized Crime* 20, no. 3–4 (December 2017): 316–37, https://doi.org/10.1007/s12117-017-9306-7.

15 Closs and McGarrell, "Enhancing Security Throughout the Supply Chain."

note that supply chain security aims to manage risk by reducing vulnerabilities in the supply chain. Risk affects two key components of an effective supply chain: reliability and resiliency. *Reliability* is defined as "the probability that a product operates properly for a given period of time."[16] *Resiliency* is defined as "the ability of a system to quickly react to the undesired events when they happen."[17] Supply chains ought to be able to substantially recover much of their capacity as part of resiliency. The COVID-19 pandemic and a general proliferation in supply chain security risks have brought all of these terms to the forefront of national and global attention. The concept of *national security* focuses on the "protection of the nation and its people from attack and other external dangers by maintaining armed forces and guarding state secrets."[18] The defence acquisitions supply chain is constantly under threat from external forces and often involves state secrets, so its protection is a national security priority.

Why do certain challenges arise in supply chain security and how can the U.S. Government, its allies, and private industry address these challenges? The increase in supply chain security risks is due to a variety of factors including: firms primarily focused on supply chain efficiency; supply chain globalisation; concentrated manufacturing and centralised distribution; increased outsourcing; and supply base reduction.[19] This is consistent with the U.S. DoD's report on supply chain integrity and its discussion of the five macro forces driving risk in the defence supply chain: sequestration and uncertainty of U.S. spending; decline of U.S. manufacturing base capabilities and capacity (due in part to outsourcing and globalisation); deleterious U.S. government business and procurement practices (that have historically prioritised efficiency); industrial policies of competitor nations; and diminishing U.S. Science, Technology, Engineering, and Mathematics (STEM) and trade skills.[20] These five macro forces contribute to ten types of risk that the defence industry often encounters. Among these, this paper will address three of the most critical risks: counterfeit and contraband goods, foreign dependency, and insufficient capacity in small and medium-sized manufacturers to ensure product integrity.

Counterfeit goods in the defence supply chain have direct and severe consequences on national security and military effectiveness. Director of the Missile Defense Agency General Patrick O'Reilly described the effect of counterfeits astonishingly well: "we do not want a $12 million missile defence interceptor's reliability compromised by a $2 counterfeit part." Indeed, a report by the U.S. Government Accountability Office details that counterfeit goods "have the potential to seriously disrupt the DoD supply chain, delay missions, and

16 Chunghun Ha, Hong-Bae Jun, and Changsoo Ok, "A Mathematical Definition and Basic Structures for Supply Chain Reliability: A Procurement Capability Perspective," *Computers & Industrial Engineering* 120 (June 2018): 334–45, https://doi.org/10.1016/j.cie.2018.04.036.

17 Claudia Colicchia, Fabrizio Dallari, and Marco Melacini, "Increasing Supply Chain Resilience in a Global Sourcing Context," *Production Planning & Control* 21, no. 7 (October 2010): 680–94, https://doi.org/10.1080/09537280903551969.

18 Holmes, "What Is National Security?"

19 Uta Jüttner, Helen Peck, and Martin Christopher, "Supply Chain Risk Management: Outlining an Agenda for Future Research," *International Journal of Logistics Research and Applications* 6, no. 4 (December 2003): 197–210, https://doi.org/10.1080/1367556031000162701 6.

20 Interagency Task Force in Fulfillment of Executive Order 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States" (Department of Defense, September 1, 2018), https://media.defense.gov/2018/oct/05/2002048904/-1/-1/1/assessing-and-strengthening-the-manufacturing-and-defense-industrial-base-and-supply-chain-resiliency.pdf.

affect the integrity of weapon systems."[21] The Senate Armed Services Committee (SASC) found in its 2012 report that there were 1,800 cases of suspect counterfeit electronic parts in the two year period from 2009 to 2010 involving over a million individual suspect parts. The Committee traced 100 of the 1,800 cases back through the supply chain and found that 70 percent of these suspect parts originated in China. The Chinese government has prosecuted many manufacturers of counterfeit goods, but Beijing remains unreliable in reducing the trade of counterfeits. U.S. government reports consistently point to China as the global epicentre of counterfeit production.[22] While it is extreme to assume that all Chinese products incur a national security risk, policymakers must be wary of dealing with Chinese firms and perform the needed due diligence.

Counterfeit parts incur a high economic burden upon firms and government agencies alike. A May 2012 report from the Senate Armed Services Committee details a case in which counterfeit goods forced the Missile Defense Agency and its contractors to invest $4.5 million in reworking costs.[23] When this multimillion dollar cost is multiplied by 1,800 over a period of just two years, the fiscal consequences are enormous. Counterfeits pose a serious risk to national and supply chain security if defective products continue to leak into the defence supply chain. It is worth noting that counterfeits can be deceptive or non-deceptive in nature, but the majority of security threats are posed by deceptive counterfeits. This risk includes the potential for intentional abuse, by state or non-state actors, in order to gain an edge over adversaries.

Foreign dependency has evolved as another type of risk to supply chain security.[24] China exports 74% of the world's personal laptop computers and two-thirds of all cell phones.[25] Beijing's "Made in China 2025" plan seeks to widen China's global lead in the manufacturing of ten key sectors, including new advanced information technology and key materials.[26] This plan is mentioned in the DoD's report on supply chain resiliency which notes that China "represents a significant and growing risk to the supply of materials and technologies deemed strategic and critical to U.S. national security."[27] In addition, it acknowledges that this particular challenge is shared by U.S. allies such as Germany and Australia and highlights the trade asymmetry that Indo-Pacific allies have with the People's Republic of China. The U.S. is completely import-reliant on 19 minerals, and any disruption in one of these minerals halts the production of defence systems such as radar and guided missiles.[28] Seventeen of these minerals are sourced from China, and are

21 Belva Martin, "Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts—ProQuest" (United States Government Accountability Office, July 12, 2010), https://www.gao.gov/new.items/d10389.pdf.

22 "Inquiry Into Counterfeit Electronic Parts In The Department of Defense Supply Chain."

23 Watson, Jillian, "Essays On Deceptive Counterfeits In Supply Chains: A Behavorial Perspective" (2015). *All Dissertations*. 1589. https://tigerprints.clemson.edu/all_dissertations/1589

24 For more information on the risk of dependency on foreign suppliers, see Theodore H. Moran, "The Globalization of America's Defense Industries: Managing the Threat of Foreign Dependence," *International Security* 15, no. 1 (1990): 57, https://doi.org/10.2307/2538982.

25 Lund et al., "Risk, Resilience, and Rebalancing in Global Value Chains | McKinsey."

26 Scott Kennedy, "Made in China 2025," Center for Strategic and International Studies, June 1, 2015, https://www.csis.org/analysis/made-china-2025.

27 "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," p. 36.

28 Marc Humphries, "China's Mineral Industry and U.S. Access to Strategic and Critical Minerals: Issues for Congress," n.d., 26.

used in other sectors of the economy such as high tech and clean energy.[29] The supply chain security risks that endanger the rare earths and minerals supply are both short and long term, but both centre around the concentration of the industry within China's borders. In addition to China's business environment appealing to many mining and mineral processing firms, China "strategically flooded the global market with rare earths at subsidised prices, [drove] out competitors, and deterred new market entrants."[30] In 2010, Beijing cut export quotas causing prices to quadruple.[31] Downstream partners were reminded of their disproportionate reliance on China for rare earths and how China could use this production as a major bargaining chip, in ways reminiscent of how the Organization of the Petroleum Exporting Countries (OPEC) manipulates oil prices to drive out competitors. Nations have previously responded with rare earth firms of their own, but many such as Molycorp were insolvent due to a series of financial failures and the sheer technical and environmental complexity associated with the industry. Molycorp was left with $1.7 billion in debt and an incomplete processing facility.[32] Export quotas like the type put in place in 2010 have been declared illegal by the World Trade Organization, but Beijing has sought an appeal.[33] Recently, China used its market leverage by sanctioning Lockheed Martin, Boeing Defense, Raytheon, and other U.S. companies for Washington's decision to sell an additional $2.4 billion in arms sales to Taiwan.[34] Previous weapon sales with Taiwan have not reduced business within China, but this action may be a precursor to future retaliation.

In addition, Beijing has threatened to create a rare earths "blacklist" if foreign companies are seen to harm Chinese interests or have links to parties that harm Chinese interests, specifically in the wake of the U.S. banning multiple Chinese tech giants from Huawei to Tencent.[35] Japanese businesses in particular could be affected, placing the Japanese government in a delicate position to walk the line between a robust alliance with the U.S. and its largest trading partner. Beijing has proven that it holds the ability and the will to tamper with this market. China is already the world's largest rare-earth consumer, and "Beijing cares less about exporting these elements for profit than feeding its high-tech industries."[36] In particular, China's fervour to dominate the market for industries such as electric vehicles could soak up so much of China's domestic supply that it would force rare

29 Jamie Smyth, "Industry Needs a Rare Earths Supply Chain Outside China," *Financial Times*, July 28, 2020, https://www.ft.com/content/fc368da6-1c86-454b-91ed-cb2727507661.

30 "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," p. 29.

31 Jamie Smyth, "US-China: Washington Revives Plans for Its Rare Earths Industry," Financial Times, September 14, 2020, https://www.ft.com/content/5104d84d-a78f-4648-b695-bd7e14c135d6.

32 June Teufel Dreyer, "China's Monopoly on Rare Earth Elements—and Why We Should Care," *Foreign Policy Research Institute*, October 7, 2020, sec. Analysis, https://www.fpri.org/article/2020/10/chinas-monopoly-on-rare-earth-elements-and-why-we-should-care/.

33 Valerie Bailey Grasso, "Rare Earth Elements in National Defense: Background, Oversight Issues, and Options for Congress," n.d., 40.

34 "China Says Will Take Necessary Measures on U.S. Arms Sales to Taiwan | Reuters," *Reuters*, October 27, 2020, https://www.reuters.com/article/us-china-usa-taiwan/china-says-will-take-necessary-measures-on-u-s-arms-sales-to-taiwan-idUSKBN27C0U0.

35 Chris Gill and Jim Pollard, "China Threatens Rare Earth Blacklist as Trade War Expands," *Asia Times Financial*, October 12, 2020, https://www.asiatimesfinancial.com/china-threatens-rare-earth-blacklist-as-trade-war-expands.

36 Lee Simmons, "Rare-Earth Market—Foreign Policy," *Foreign Policy*, July 12, 2016, https://foreignpolicy.com/2016/07/12/decoder-rare-earth-market-tech-defense-clean-energy-china-trade/.

earth dependent nations to look elsewhere for sourcing these materials. Global demand is already set to continue to increase based on historical projections, but the worldwide initiative to eliminate carbon emissions may increase demand at an even faster rate due to higher production of wind turbines and electric vehicles.[37] Even if Beijing never used its supply dominance for intentional acts of economic statecraft, the global economic dependence on a sole source for rare earth elements poses a supply chain risk. Supply chain security risks ranging from natural disasters to cyberattacks could choke this sort of "single point of failure in China," crippling downstream industry.[38]

The Department of Defense also identifies a third risk that threatens supply chains. Under Secretary of Defense for Acquisition and Sustainment Ellen Lord testified to the Senate Armed Services Committee in October 2020 concerning many topics regarding defence acquisition supply chains. She highlighted the role that small and medium-sized businesses play in the defence supply chain, citing that 24.2% of the entire DoD budget, or $75.4 billion, was directed toward small businesses in 2019.[39] Additionally, subcontract funding in the same year was $62.3 billion meaning that there was "significant flow down from major defence primes to small businesses."[40] Incorporating small businesses into the defence supply chain reinforces the notion that small businesses are "the backbone of the American economy," but they can be a major liability in the supply chain. Many of these small to medium-sized enterprises (SMEs) are at a small scale or are rapidly growing, so cash profits are needed to sustain operations or continued growth. These firms prioritise economic efficiency, and rightfully so. However, if these SMEs neglect security, then they could jeopardise the integrity of the broader supply chain.[41] Manufacturers are of particular concern since 99% of the 347,000 manufacturers in the U.S. are small and medium-sized and 50% of those lack basic cyber controls. Yet manufacturers "received the greatest volume of targeted cyber-attacks of all industries globally" in 2014.[42] Due to their small scale, "many small and medium-sized manufacturers are unaware of federal requirements and may lack the financial and technical capabilities required to manage cybersecurity risks," thus introducing considerable risk.[43] Financially, these suppliers lack adequate scale to bear substantial fixed security costs. While larger firms can spread those fixed costs for security over a much larger enterprise, smaller firms often lack the resources or expertise to adequately secure their operations. As a result, poorly protected manufacturing suppliers pass their vulnerabilities on to larger corporations, and eventually, the defence acquisitions supply chain.

37 Simmons, "Rare-Earth Market—Foreign Policy."

38 Smyth, "US-China."

39 David Vergun, "DOD Supports Small Businesses in Big Ways," U.S. Department of Defense, October 1, 2020, https://www.defense.gov/Explore/News/Article/Article/2368903/dod-supports-small-businesses-in-big-ways/.

40 Ellen Lord, Defense Department Supply Chain Readiness and Integrity | C-SPAN.org, Congressional Hearing (C-SPAN), October 1, 2020, https://www.c-span.org/video/?476435-1/defense-department-supply-chain-readiness-integrity.

41 For a more comprehensive analysis on SMEs and risk management, see Chiara Verbano and Karen Venturini, "Managing Risks in SMEs: A Literature Review and Research Agenda," *Journal of Technology Management & Innovation* 8, no. 3 (2013): 33–34, https://doi.org/10.4067/S0718-27242013000400017.

42 "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," p. 51.

43 Ibid, p. 88.

Contracting and subcontracting are both common in modern manufacturing. 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.[44] This "multi-tiered" structure makes it difficult to ensure the security of the supply chain since third and fourth-tier suppliers tend to be much smaller and more specialised than first and second-tier suppliers. These third-party suppliers may further outsource certain components or operations, thus creating "fourth-party" suppliers.[45] This leads to another problem in the supply chain that exacerbates the issue of insecure smaller firms: transparency. Transparency, or visibility as McKinsey refers to it, represents "the extent to which [a] customer can trace spending at [a] subtier level."[46] The more complex the supply chain, the more subtiers there are and the more difficult it is to actually track sources of risks and vulnerabilities. A vulnerable SME could possibly never be identified depending on the complexity of the supply chain. For example, if a defence acquisitions supply chain incorporated Chinese firms that were influenced directly by the Chinese Communist Party (CCP), suppliers could deliberately or inadvertently contribute to foreign espionage efforts by fielding vulnerable security systems or sharing sensitive information with other businesses or state-run entities. The pervasive presence of the Chinese Communist Party in China's domestic political economic landscape provides considerable access and influence within many Chinese companies. Such sway can influence the incentives facing Chinese suppliers. Lawsuits, intellectual property theft, exploited information security vulnerabilities, and any unlawful activities of opaque third- and fourth-party suppliers ultimately place downstream partners at risk. Addressing such violations once they have occurred can lead to operational delays, compromised brand integrity, and considerable losses of time and money. This diminishes the reliability of supply chains, often reducing their performance. If defence supply chains are reduced in performance, then the military may be unable to receive sustainment or reliable equipment thus imperilling national security. A market-based risk system for assessing risk could help identify and monitor threats to supply chain security.

Defective counterfeit goods, dependency on foreign entities, and a lack of security infrastructure in SMEs are all current supply chain security risks that confront the defence industrial base. For each risk, there are many actions the U.S. government can take. Congress can impose tighter restrictions on products from subcontractors, and subsidise the onshoring or nearshoring of supply chains to enhance visibility and control. It can begin a national stockpile of rare earth minerals in the case of an emergency drop in global supply, and diversify suppliers by investing in market-based solutions domestically and within allied nations. It can require the auditing of certain tiered suppliers, and support SMEs in cybersecurity strategies. While all of these measures are valid, they miss the crucial heart of the issue behind supply chain risk management. Governments cannot adequately manage supply chain risk alone. The decade-long failure to establish and maintain a U.S.-based rare earth minerals market is just one example of challenges facing government efforts to address these supply chain security

44 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#.

45 Kaushik Sen, "What Is Fourth Party Risk?," UpGuard, November 14, 2019, https://www.upguard.com/blog/what-is-fourth-party-risk.

46 Lund et al., "Risk, Resilience, and Rebalancing in Global Value Chains | McKinsey."

challenges. New industries, innovations, and new technologies will continually introduce new challenges that perennially outpace the regulatory and monitoring capacity of legislatures and bureaucracies. The U.S. government failed to detect and mitigate the systemic financial risk leading up to the Great Recession of 2008. The Senate Banking and Finance Committee's inability to understand the complexity of the financial industry it was tasked to regulate was a crucial underlying reason for this failure. Too often, regulatory actions fail to keep pace with industry developments. Government responses tend to be reactive, *ex post* adjustments in the wake of revealed vulnerabilities; the equivalent of shutting the door after the horse has left the stable.

The market alone also fails to adequately regulate supply chain risk because it often waits until risks are realised (manifesting as delays and disruptions) before meting out penalties. Risks are often interconnected, and an action can exacerbate another risk if unaddressed. "Many companies develop plans to protect against recurrent, low-impact risks in their supply chains" but most "all but ignore high-impact, low-likelihood risks."[47] Larger companies often mitigate this risk by holding excess inventory or diversifying their suppliers, but these are topical solutions that create new problems. Holding excess inventory increases costs and hurts the bottom line. Diversifying suppliers creates substitutes and redundancies in the case of a disruption or delay but lengthens the supply chain and multiplies the potential number of breach points or vulnerabilities. Although these actions may improve supply chain security in the short term, they are not a comprehensive solution. There is a growing need for a broader system that utilises public-private partnerships to quantify risks to supply chain security. The public or private sector alone cannot achieve this feat, but a partnership between the two can. Such a robust system of assessment would, ideally, incentivise companies to improve their risk profile by engaging in the best security-enhancing measures available given specific risks and circumstances.

Supply chain risk management is vital to preserving national security for both America and her allies. As discussed in more detail below, such a market-oriented risk assessment system could function in a manner similar to the FICO personal credit score system prominent in the United States. Assigning scores based on a dynamic and evolving set of security criteria would enable companies to proactively uncover supply chain security weaknesses while also incentivising them to improve their scores by taking measures to improve the most vulnerable parts of their supply chains. Although many sectors could eventually benefit from such a risk assessment system, the defence acquisitions industry will likely see the most immediate and direct security benefits from implementing this sort of system.

47 Sunil Chopra and ManMohan Sodhi, "Managing Risk To Avoid Supply-Chain Breakdown," MIT Sloan Management Review (MIT Sloan School of Management, October 1, 2004), http://www.tlog.lth.se/fileadmin/tlog/Managing_Risk_to_Avoid_Supply-Chain_Breakdown.pdf.

The Supply Chain Security Risk Assessing System

How A Risk Assessing System Would Work

The current FICO system is the premier way to assess and quantify consumer credit risk and is used in over ninety percent of lending decisions in the United States, making it indispensable in the banking industry and other subsectors of the financial world.[48] Scores are based on a variety of factors that have been shown over time to correlate with credit worthiness. The FICO system operates with a combination of five predetermined factors that underpin an overall score that is used as the prime indicator of consumer credit risk.[49] Each of these components has a corresponding weight in determining the overall score which can change over time depending on an individual's financial position and activities.[50] Although in any individual case such assessments may not be perfectly accurate, in aggregate such scoring has proven to be a fairly reliable indicator of credit risk. Over time, risk rating agencies have gathered a large body of consumer financial data that has helped sharpen the algorithms they use to measure credit risk.

The business of generating such scores falls to several credit agencies. Consumer credit agencies maintain proprietary systems and standards for evaluating individual credit risk. A notable feature of the FICO score is that it may be slightly different from one rating agency to another. A FICO score may not be the exact same between Equifax and Experian, for instance, due to nuanced differences in those companies' algorithms and length of credit history used.[51] This generates a degree of competition for the provision of accurate risk assessment. By vesting multiple rating agencies with the ability to measure credit risk, there is a cumulative effect of incentivising the continual refinement of assessment tools. The FICO system has led to greater transparency and more financial awareness by Americans and American businesses, thus creating an improved system for the protection of the financial industry and a high level of efficiency in the allocation of consumer credit.

A system inspired by the FICO credit scoring system can be applied to assess individual firms' supply chain risks. Just as individual consumer credit risk can be measured and quantified, we propose a system to quantify and measure firms' supply chain risk. This system would entail multiple supply chain risk assessing agencies. Some of these should be private entities who would sell their assessments on a for-profit basis in the same fashion as consumer credit rating agencies. Such rating agencies could also potentially be non-profit bodies or public entities. Each of these types of adjudicating entities might work in slightly different ways, with differing incentive structures and approaches to the task of measuring supply chain security risk. An industry association sponsored

48 Tatiana Homonoff, Rourke L. OBrien, and Abigail B. Sussman, "Does Knowing Your FICO Score Change Financial Behavior? Evidence from a Field Experiment with Student Loan Borrowers," *SSRN Electronic Journal*, 2018, https://doi.org/10.2139/ssrn.3129075.

49 These five factors include the categories of new credit, length of credit history, credit mix, payment history, and amounts owed.

50 "How Are FICO Scores Calculated? | MyFICO | MyFICO," accessed July 25, 2020, https://www.myfico.com/credit-education/whats-in-your-credit-score.

51 Elizabeth Spencer, "Why Your Credit Score Is Different Depending On Where You Look," Money Under 30, September 22, 2019, https://www.moneyunder30.com/why-is-my-credit-score-different-depending-where-i-look.

non-profit might be more attuned to key predictors of risk than a more generalist adjudicating entity. But perhaps the more broadly based profit-oriented entity produces more accurate algorithms based on a larger underlying base of data. Or perhaps a congressionally-mandated entity achieves higher levels of compliance and elicits broader cooperation from firms. At the outset, it is difficult to know which type of entity would be most effective. Given the uncertainty and since this approach to supply chain risk assessment is a novel concept, we might suggest starting with several different types of models (private, public, and non-profit adjudicating bodies) and allowing time and market dynamics to judge which sort of structure generates the best results. Risk assessing agencies can develop scoring algorithms by processing data related to previous and ongoing problems in supply chain security. Such observations could train these algorithms to more accurately assess risks and forecast damages. Over time, these algorithms could harness positive track records of supply chain reliability as well as negative experiences of supply chain failures to improve risk detection.

The system we are proposing would seek to apply insurance firms and actuaries' risk assessment to firm-specific supply chain risk. Supply chain risk scores can be based on objective algorithms that incorporate factors such as number and location of upstream suppliers. These algorithms will produce a supply chain risk score that is within a fixed range (like a credit score) and weighted in relation to other risk factors.[52] Collaboration between insurance agencies, risk pricing agencies, and the DoD's in-house risk modelling may be necessary for effective quantification of risk. Over time, the algorithms can be sharpened and adjusted as additional data is gathered. Through this system, businesses and consumers (including the DoD) could dramatically improve their understanding of supply chain risk exposure at a relatively low cost.

Multiple risk rating agencies would compete against one another to develop algorithms that employ the optimal combination of factors for measuring risk. The reality is that Congress, specific industry associations, insurance companies, or supply chain risk experts are each likely to have very different approaches to what constitutes the most accurate way to measure supply chain security risk. This heterogeneity is a source of strength under initial conditions of uncertainty about what factors will actually prove most beneficial for indicating risk. Over time as security breaches or other supply chain failures come to light, the relative performance of particular adjudicating entities (and their associated algorithms) should emerge. Eventually, stronger performers should consolidate the space, achieving natural scale advantages. But initially, we suggest allowing multiple types of adjudicating entities fielding a diverse range of risk algorithms to compete. Relying on competition to develop this system is an efficient, market-oriented way to cultivate the most accurate risk assessment metrics in the shortest amount of time. Additionally, these companies can work with various industries to delineate the unique challenges they face and how those challenges should be evaluated when determining risk scores. The main weights and factors of scoring algorithms can be revealed to the public and to firms to encourage efforts to improve supply chain security, but specific details will remain the intellectual property of the risk assessing agencies.

52 For a methodological example of how risk indices can be used to quantitatively measure risk in the defence industry, see A. Trevor Thrall and Jordan Cohen, "2020 Arms Sales Risk Index," (Cato Institute, October 27, 2020), https://www.cato.org/publications/e-publications/2020-arms-sales-risk-index#mapping-risk.

This sort of supply chain risk score could be shared with the public and stakeholders. Firms that have worked hard to secure their supply chain will gain a competitive advantage. Savvy consumers could consider risk scores when deciding among potential suppliers. Such public visibility would incentivise firms to correct their supply chain vulnerabilities and insulate themselves from security risks. The impact would be more proactive internalisation of the costs of potential supply chain disruption and security breaches. In addition, information sharing enables capital markets to react negatively to firms that do not improve their supply chain security or have excessive amounts of risk. Competing for certain types of contracts could require that bidders meet minimum scores. Therefore, businesses will be inclined to bolster their supply chain security in order to improve their scores over time. Publicly traded firms would be inclined to reduce supply chain security risk in order to satisfy current stakeholders or potential ones. The supply chain risk score could be disclosed to the public in the annual 10-K financial statement.[53] Such disclosure would compel companies to be more conscious of supply chain security and be more transparent with investors. A heightened sense of accountability and apprehension would benefit all parties involved and would expand resiliency in the long run.

It would be a fairly natural extension to move from risk assessment and quantification to pricing such risk. Once supply risk can be reliably quantified, a secondary market could develop for insuring supply chain risk. One could easily imagine supply chain risk insurance being priced as a function of a firm's quantified risk assessment. In addition to taking measures to enhance their supply chain security, firms could also opt to buy supply chain risk insurance. Alternatively, firms with secure supply chains will save on insurance costs. Downstream consumers and partners might demand that poorly scoring suppliers provide third party insurance guarantees to offset their exposure to demonstrable supply chain risks. Eventually, risk aggregators could emerge. Assuming that individual companies' supply chain risks could be productively aggregated in a non-correlated fashion (which, as the 2007/2008 housing crisis showed, may prove harder to do in practice than in theory), brokering entities could provide further benefits of reduced system risk and sectoral resiliency for individual supply chains.

Advantages of a Risk Assessing System

There are four major advantages to this proposed supply chain security risk assessing system. First, the system leverages free market dynamics by harnessing competition to catalyse the development and continual improvement of risk pricing algorithms. Having multiple types of adjudicating bodies structured in different ways (for-profit, governmental, non-profit, sectoral-specific, and generalist) should foster competitive dynamics. Competition will improve accuracy and enhance system-wide security. Under this system, capital markets and informed consumer behaviour can scrutinise firms with excessive or non-transparent supply chain risk. Ratings firms will be incubators of innovation as they fine-tune precise adjustments for the assessment metrics. Today, supply chain vulnerabilities often remain undetected or unappreciated until after a breach

53 The Form 10-K is an annual report that publicly-traded companies are required by law to file in the U.S. with the Securities and Exchanges Commission (SEC). It provides a comprehensive overview of a company's financial condition by including audited financial statements. This form is sent to shareholders annually before they elect the company directors, and is also publicly available so potential investors can determine whether to buy or sell shares of a company or invest in corporate bonds.

or failure is exposed. Complex, global supply chains are difficult to map and proactively evaluate. Under such conditions of uncertainty, we believe a creative, market-oriented approach instilled with competitive innovation offers substantial benefits over a static, often *ex post* regulatory solution for supply chain security. By dividing risk assessment duties across multiple private entities, we provide for both competition and innovation while also minimising the likelihood of capture by powerful sectors or firms. Independent rating agencies with proprietary algorithms and processes for judging supply chain risk also make it difficult for firm executives or employees to interfere with risk assessments.

The second advantage of this sort of market-oriented risk assessment system is the opportunity it provides for firms to address shortcomings in their supply chain vulnerabilities both directly (by eliminating sources of risk) and indirectly (by seeking third party insurance). Although supply chain risk assessment will incentivise firms to take actions that improve their supply chain security, this dynamic could take time to develop. To help cover the gap between the reality of where a particular supply chain finds itself and where partners would like it to be, we suggest that an insurance mechanism also be created. Such insurance could leverage supply chain risk scores to price and design risk mitigating insurance products. If risk is quantified and companies are insured, then supply chains will become more resilient and downstream damages limited. A new market for risk insurance will not only provide coverage for risky firms, but will educate them and incentivise firms to remediate risk. Collaboration among customers, suppliers, risk assessment entities and insurance can provide insight about the nature and location of risk and the necessary steps to reduce or eliminate it.

Third, this solution capitalises on government demand for reliable information on supply chain risk to foster cooperation between the public and private sectors. The public sector's demand for supply chain integrity, particularly in the national security domain, can inspire new entrepreneurship. The defence-oriented solutions we are suggesting may also gain traction in industries outside of defence acquisitions. Other industries like the pharmaceutical industry are also likely to be interested in mitigating their supply chain risks. The eventual expansion of this system to other industries remains another attractive benefit.

A final advantage of this proposal is that ratings agencies should only require light-touch regulation from the federal government in order to maximise the efficacy of the system. Rather than require an intrusive regulatory footprint to ensure supply chain integrity, or burden a wide range of firms with onerous compliance requirements, this system would rely on market mechanisms to ensure reliable supply chains. This sort of system would rest on the microeconomic optimisation behaviours of individual firms responding to internalised costs of risk in their supply chains that today are either largely exogenous or deferred until a catastrophic breach turns risk into realised loss. Incorporating a supply chain risk score into auditing will help shareholders and auditors to better understand supply chain security risk and incentivise companies to actively manage the health of their supply chains. Maintaining excellence in their supply chains will benefit the firm and shareholders alike. Protecting their score would incentivise firms to self-police against opaque or illegal activity performed by suppliers. For the most part, such behaviour is motivated by concern over their brand and public image in an industry where much of firm value resides in such intangible assets. This same dynamic of cost internalisation can be applied to supply chain risks more broadly.

Challenges

In this section, we address five specific challenges for both policymakers and businesses in implementing a FICO-like risk-assessing scheme: the exit of rated firms from defence markets and subsequent suppression of competition; the disproportionate burden borne by small and medium enterprises; the possibility of perverse incentives; the risks of regulatory arbitrage; and the difficulties of implementing the system internationally.

For businesses, one of the primary challenges is the deterrent effect that new regulation or compliance requirements might have on a subset or the entirety of an industry. This risk assessment system might dissuade companies from competing for public contracts. This effect would be particularly undesirable in the defence acquisition realm where competition is already somewhat limited. Any company that buys into this scoring system and is rated poorly may be deterred from participating in future defence contracts, thus decreasing competition among bidders and reducing product availability in the defence acquisitions process. The supply chain risk insurance system, if properly implemented, could help protect the defence acquisitions space from this chilling effect. If a company is rated poorly, supply chain risk insurance could help offset supply chain risk in the short term while the company implements measures to improve its supply chain risk profile. In the long term, however, that same company would be motivated to improve its supply chain security to reduce insurance costs and to compete better for bids.

Another challenge is that improving supply chain security risk scores would be relatively more expensive for small- and medium-sized enterprises (SMEs). Whether it is stronger cybersecurity architecture, legal fees related to conducting due diligence on potential international suppliers, or premiums of supply chain risk insurance, such fixed costs are spread over a much smaller revenue base for SMEs. Although this system would put additional pressure on SME suppliers, it could also become a source of comparative advantage for firms that demonstrate a dedication to supply chain security. For customers that prefer a wider pool of partners (even if that entails some additional supply chain risk), they could elect to be less stringent in the supply chain security ratings requirements of potential suppliers.

Although the supply chain risk assessment system's application will prove beneficial for the supply chains of all companies, regardless of size, it will be especially impactful for these SMEs. It is imperative that small businesses are provided with the opportunity to obtain both a FICO-like supply chain risk rating and supply chain risk insurance to compensate for their lack of capacity. Congress should consider creating a pool of funds for qualified third- and fourth-tier suppliers in the national security arena. Such funds could be used to directly shore up supply chain vulnerabilities or to purchase insurance against such risks. This solution will guarantee vital defence contractors the funds they require to secure their supply chains and, thus, ensure the integrity of the defence acquisition supply chain.

One problem that plagues all regulatory regimes is perverse incentives: incentives that motivate actors to behave contrary to the intent of regulators. Secrecy can help alleviate this problem. One of the reasons that the FICO credit score system is so effective at rating individuals' risk profiles is that the exact algorithms for determining credit scores are proprietary and kept secret from consumers and other credit agencies alike to maintain competitive advantage. Granted, these algorithms are not *completely* secret.

Credit scoring companies still provide consumers with general guidelines for how to improve their credit scores, for example: obtain a longer credit history, pay your bills on time, use a smaller proportion of your available credit, etc. Such moves toward personal fiscal responsibility is not a bad outcome. In fact, if suppliers took measures to lower their risk, that would be a positive consequence of supply chain security risk scoring.

Regulatory arbitrage, or taking advantage of loopholes and weaknesses in regulation to extract optimum outcomes, is another challenge for implementing supply chain risk assessing. The farther removed a firm is in the supply chain, the more difficult it is to inspect and the easier it is for firms to lie about or otherwise circumvent supply chain security measures. This is especially true for international supply chains that cross multiple jurisdictions. Though this problem is far from simple, a partial solution involves progressively pricing supply chain unknowns. More specifically, a company's risk profile will be worse and that company will be less likely to secure a defence tender if that firm is less subject to U.S. regulatory enforcement, more exposed to contradictory foreign regulations, or providing less verifiable information regarding supply chain risks. Put simply, more unknowns in a supply chain yields worse risk ratings for involved firms.

Though the risk in such unknowns should be factored into supply chain risk profiles, prudence dictates that regulators must accept some level of uncertainty in international supply chains, given the heavily distributed nature of modern supply lines. International cooperation on creating and implementing this risk rating system, however, could reduce this inherent uncertainty. If the United States joined with long-term allies like the United Kingdom, Israel, Australia, or South Korea to implement and harmonise the risk profile and risk insurance systems, regulatory blindspots would significantly shrink as monitoring capabilities multiplied. Although the ideas in this article have been presented in a largely U.S. empirical context, the supply chain risk assessment system that we are proposing could also be implemented across many partner and allied states in the Asia Pacific region. Of course, noncompliant states could impede monitoring and enforcement. One such example is China, a country notorious for refusing foreign inspections of domestic facilities, falsifying domestic inspections of those same facilities, and miring businesses in the red tape of unwritten protocols for business-government interactions. There is little the United States or its allies can do to change regulatory deficiencies in such countries, so risk assessing entities would likely have to learn by trial and error, assessing risk for supply chains operating in these locales and deftly adjusting risk algorithms as supply chain security incidents occur. A conservative approach to pricing such risks is advisable.

Conclusion

Defective counterfeit products, foreign dependency in critical industries, and insufficient security infrastructure and opaqueness are just a few of challenges plaguing the supply chains of modern businesses. If supply chain security vulnerabilities are not identified and addressed, industries will suffer. Defence industries, in particular, must take action against external and internal supply chain risks to streamline procurement processes and, more importantly, protect national security and the health of the defence-industrial base. A supply chain risk assessment system akin to the FICO consumer credit scoring system would address these concerns by leveraging free market competition among risk assessment agencies to price supply chain risk in complex, international industries.

Our proposal lays the foundation for continuous improvement and innovation in supply chain risk assessing algorithms, suggests an agile insurance industry for providing coverage to defence procurers, and provides alternatives for smaller suppliers to secure otherwise vulnerable supply chains. Additionally, the system increases accountability and transparency for all stakeholders by quantifying supply chain risk. Though not without its challenges, implementation of such a market-oriented approach should bolster national security and help maintain a robust defence-industrial base. This article is unlikely to be the final word on supply chain security challenges, but we hope to stimulate a useful discussion on the merits and potential mechanisms for addressing some of these challenges.

William Norris is Associate Professor in the Bush School of Government and Director of the Economic Statecraft Program (ESP) at Texas A&M University. Chase Blazek is a Program Aide and holds a Master of International Affairs from the Bush School. Joseph Rodgers, Tarni Hewage, and Braeden Kobza are Research Assistants for ESP.