SYM-AM-21-107

Excerpt from the Proceedings of the Eighteenth Annual Acquisition Research Symposium

Quantifying Systemic Risk and Fragility in the U.S. Defense Industrial Base

May 11–13, 2021

Published: May 10, 2021

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Quantifying Systemic Risk and Fragility in the U.S. Defense Industrial Base

John Ullrich—is pursuing a Doctor of Engineering degree in engineering management from the George Washington University. He holds a Master of Systems Engineering degree from Johns Hopkins University and an undergraduate degree in packaging engineering from the University of Wisconsin–Stout. Ullrich is a Senior Program Manager in Global Supply Chain Management at Raytheon Technologies, supporting Land Warfare and Air Defense systems. Additionally, he teaches within the Systems and Industrial Engineering Department at the University of Arizona. His research interests include engineering management, C5ISR, and high-energy physics. Ullrich is a member of the American Physical Society and the International Council on Systems Engineering. [ullrich@email.arizona.edu]

John Kamp—received a Doctor of Engineering degree in engineering management from the George Washington University in 2019, a Master of Engineering degree in nuclear engineering from Iowa State University, and a Bachelor of Arts degree in mathematics and French from the University of Nebraska–Lincoln. Kamp joined the George Washington University research staff in 2019 and supports Dr. Etemadi's acquisition strategy research project. He is a retired naval submarine officer with extensive experience in research and development and program management. His research interests include engineering management, maritime systems, and acquisition system research. Kamp is a Fellow in the Royal Institution of Naval Architects and a member of several professional associations. [jckamp2018@gwu.edu]

Abstract

This research quantifies fragility within the U.S. Defense Industrial Base (DIB) and translates it into supplier risk. The proposed model identifies systemically critical suppliers, where critically is characterized in terms of the supplier either being highly coupled within the industrial base, operating in a limited competition space, or owning a disproportionately large market share within a specific commodity. Each of these properties is quantified using centrality and community detection methods. By correctly assessing critical suppliers in the defense base, it allows for a methodical approach to addressing standard failure modes that typically result in material disruptions in advance of realizing interruptions. Quantifying fragility in supply chains based on systemic centrality and communities is a novel effort. Direct application of this process within the DIB fundamentally approaches assessing and strengthening our supply base resiliency in a completely different manner.

Keywords: Defense Industrial Base, Fragility, Centrality, Community Detection, Systemic Risk

Introduction

The U.S. Defense Industrial Base (DIB) comprises a massive network of suppliers who, in totality, offer the capabilities and capacities required to meet and sustain the demand for the raw material, components, subsystems, and end-item deliverable weapon systems. Government agencies have focused on quantifying multiple dimensions of supply base risk within the DIB. In general terms, risk in this context is the uncertainty of events that would disrupt the material flow or create system availability delays. The U.S. Government Accountability Office (GAO) has provided multiple reports to the House of Representatives Committee on Armed Services recommending quantification methodologies and practices to manage supply base risk within the DIB (GAO, 2017). There is a two-part challenge in undertaking the effective execution of supply chain risk management within this environment. First, the DIB is supporting a range of diverse products and technologies. Secondly, traditional supply-chain risk management approaches focus on programmatic impacts versus systemic impacts (Sinha et al., 2004). The Department of Defense (DoD) Critical Asset Identification Process (CAIP) quantifies Task Critical Assets (TCA) annually (DoD, 2008). For material considered defense-critical or task-critical by the DoD, the rough cost and schedule impact to requalify an unknown supply source is as high as $10 million and 9 months.

To illustrate the challenges of criticality assessment and program-centric supplier risk focus, consider a sole-source of supply for precision machined parts. One of the critical risk characteristics the GAO identifies is sole source dependencies (only one qualified source). In this hypothetical scenario, suppose that our sole source of supply were to declare bankruptcy and immediately cease operations. Programmatic consequences manifest as unfavorable impacts to cost, schedule, or both. The first realized consequence manifests as a limitation of manufacturing at the system level to the material on-hand position. This degraded state persists until a qualified alternative source of supply can be established. The total impact will directly correlate with the material's complexity and relative criticality to system-level operational requirements. Suppose this supply source is limited to a single program. In that case, the impact is limited to the cost and schedule associated with requalification. In this example, identifying criticality and risk consequence is program-facing; there is no accounting for more extensive dependencies or consequences within the DoD.

In contrast, consider the same bankruptcy scenario with a tightly coupled supplier within the DIB, meaning multiple programs provide manufacturing demand to the supplier. Connecting demand amplifies the impact of supply loss across programs, prime contractors, defense agencies, and, ultimately, throughout an entire commodity (North American Industry Classification System [NAICS]). Government program offices have limited information on single sources of supply. This research provides a pragmatic approach to quantifying a supplier's criticality within the DIB relative to its potential negative impact within the defense acquisition spectrum and utilizes network analysis to visualize and quantify dependencies within the DIB, translating them into system-risk measures.

Literature Review

Existing principles, practices, and analytic tools support this research and allow open-source spending data to characterize dependencies and connectedness and quantify fragility in terms of systemic risk. Doing so supports two novel approaches to assessing and strengthening our industrial base. First, this approach quantifies the growing dependencies within the industrial base, supporting risk management of items like obsolescence, capacity, and availability. Second, it allows for a meta-level view of the DIB that supports dynamic modeling and simulation of supplier failure propagation through the network (Meyer et al., 2014).

Fragility and System Risk Within the Defense Industrial Base

We define fragility within the DIB's context as the impact of a failing supplier on other suppliers, where failing is any disruption in material flow (availability or capacity). The current DIB is a fragile network, less conducive to competition, and challenged to scale quickly, grow, or innovate (Aviles & Sleeper, 2016). In this sense, fragility manifests as a common-mode failure where causal effects leading to failures propagate through the supply chain network. These common-mode failures can come from a range of realized impacts stemming from a range of macro forces impacting the DIB: reliance on sole-sourcing, uncertainty in defense budgets, and "bull-whip" demand cycles. These forces are quantified in terms of risk and realized as network fragility before the systemic disruption. Additionally, these forces are fundamental to creating uncertainty that stifles industry investment and growth (DoD, 2018).

While not ideal from a resiliency standpoint, supplier fragility does not directly quantify the respective supplier's risk (Lambert & Cooper, 2000), which means being a critical supplier within the DIB is not necessarily a direct indication or a probability that the supplier may fail. However, tight coupling or high dependencies within the network are a way to characterize the consequence of a respective supplier failing, most notably in terms of material disruption. Disruptions in material flow represent systemic risk, where systemic risk is the uncertainty of DIB network disruption. Moreover, realized consequence is associated with the supply base being unable to perform at total capacity or efficiency. As stated, there is a shared failure mode associated with disruption; the consequences, however, map to multiple dimensions; fragility quantification must adequately discern these modes. In this view, the DIB is not dissimilar to a complex social network or a financial network. Understanding the potential influence of a supplier within a network is a viable strategy to both modernize the industrial base and ensure a continuous supply for Defense procurement.

Traditional Network Analysis Applicability

Quantifying critical firm financial network analysis provides a pragmatic and scalable approach for defining critical suppliers and dependencies in a supply chain. Jorge Chan-Lau (2018) offered a risk-dimension mapping framework to quantify systemic risk within a financial network. Chan-Lau suggested three dimensions: first, *"too-connected-to-fail,"* where a tightly coupled firm's failure represented a risk to its neighboring firms; second, *"too-important-to-fail,"* where failure represents a considerable impact, even if the system-wide impact is not significant; and finally, *"too-big-to-fail,"* where the firm has a disproportionally large share of the systemic activities (Chan-Lau, 2018). This proposed architecture aligns well to supply chain mapping, as within the DIB supply chain, there is a range of highly connected, niche capability or massive suppliers.

Characterization of Supply Chain Risk

Supply chain risk management (SCRM) relates to the strategic management approach of risks, issues, and opportunities impacting a supply chain based on an organizational approach to assessing a respective event's potential consequences (Hallikas, 2004). SCRM directly leverages risk management tools in collaboration with supply chain professionals, both internally and externally. They focus on translating uncertainties of logistic and material flow efforts, material availability, or resources into an actionable plan for execution. Supply chain networks are inherently complex and dynamic; therefore, SCRM frameworks focus on providing effective risk management over a broad operational environment. Fundamentally, SCRM is the principle that an enterprise needs to prevent material disruptions throughout its entire supply base or supply chain. Critical measures of effectiveness are a systematic means to identify potential disruption sources, an enterprise approach to be an assessment of internal supply chain risks as well as an assessment of supplier or sub-tier supplier risk, assigned cognizant supply chain professionals managing identified risk, and, finally, the systematic means for continuous monitoring of disruptions or disruption sources (Blackhurst et al., 2008).

By definition, a supply chain inherently relies on connected critical providers, knowledge points, or handoffs, where a failure within the chain disrupts its coupled partner. In each respective reliance, uncertainty manifests as vulnerability; SCRM reduces vulnerability throughout a supply chain's entire value stream (Hallikas, 2004). Supply chain risk exists in multiple dimensions: natural disasters, raw material shortages, market forces, distribution challenges, or product or part technical maturity. This broad range of risks translates into a considerable exposure position that scales with the enterprise's size and complexity (Finch, 2004). SCRM typically incorporates the following processes as part of the risk management framework: identification, assessment, mitigation, acceptance, and monitoring of supply chain risks (Chopra & Meindl, 2009). It is a relatively heterogeneous literature base for SCRM, and the majority rely on traditional risk measures to influence action that can improve the agility or robustness of a supply chain. Supply chain agility is the speed an enterprise can react with should disruption or threat emerge within the supply base.

Quantifying this measure is the manufacturing lead time for supplier material, where minimizing the make-span or procurement-span for the material is optimal. Also included in supply chain agility is the responsiveness to changing to market needs, where an organizational goal is to build a supply base capable of transition to a different or modified material solution without impacting delivery reliability. Supply chain robustness shares some similarities with supply chain agility, where the notable delta is not an organization's ability to adapt but rather the quantified incurred disruption of a singular event. In a robust supply chain, when a change occurs, the supply base inherently provides more time to plan a course of action. Additionally, a supply chain's robustness measures a supply chain's ability to carry out its functions in a degraded state. Using a major natural disaster as an example of a disruptor, if an impacted supply base can maintain deliveries without a strategic shift in execution, it would be fair to say that the base was robust and not impacted by a singular event.

Quantification of supply chain risk is the product of a consequence in terms of an event's cost impact or material disruption incurring schedule increase compared against the event's likelihood. Like traditional risk management approaches, this product approach prioritizes and characterizes the risk and opportunity spectrum (Hubbard, 2009). This approach is the most popular methodology for quantifying risk, both within a supply chain and in the broader sense of risk management. Regardless of this approach's debatable effectiveness, it is, as stated, widely accepted within supply chain professional organizations (Manuj & Mentzer, 2008).

Factors likely to disrupt a supplier, product, program, or service establish risk archetypes; these archetypes help suggest the likelihood of impact realization (Outdot, 2010). Traditional supply chain measures supporting this quantification are a supplier's financial viability, operational capacity or expertise, or a quantifiable supplier resiliency score. Additionally, certifications provided by compliance organizations such as ISO or the National Aerospace and Defense Contractors Accreditation Program (NADCAP) indicate a low likelihood of an adverse event occurring via a supplier's successful acquisition retainment of certification. Finally, quantification of supply chain risk in customer value is germane in industry practice, where the primary measure is on-time delivery and order correctness. Supply chains with risk in a customer value dimension manage threats associated with procuring the wrong or defective products within their demand portfolio (Nishat, 2006). This risk dimension aligns with traditional measures of quality management systems: defects per unit, the accuracy of an order, or rework cycles (Rao & Goldsby, 2009).

Centrality and Community Measures of Criticality

Provided a sufficiently complex network exists, there will inherently be relationships of either highly connected nodes or tightly coupled nodes within a localized area (Newman, 2008). The well-defined principles and power laws that support these concepts stem from social network analysis and are both long-standing and proven (Bonacich, 1987). There is a nearly endless amount of research available where the application of centrality measures supports critical nodes or vertices identification within a network for a range of practical purposes, most notably the continued evolution of the use case of modeling influence in a social network (Wang & Street, 2015). Beyond social networks, these methods are in use in biology research to identify critical species in pollination communities (González et al., 2010), in health research to assess associations between measures of network centrality and health in a retirement community (Schafer, 2011), and within the financial industry to identify and assess the risk of financial firms (Chan-Lau, 2018). The common link in each application's approach is a need to understand the network's relationships that support the characterization of node importance or insignificance.

Centrality and community indices directly answer what is fundamentally important to a node, vertex, or network. The output is a tangible function providing real-values for node and flow importance concerning the analyzed network. As stated previously, the word “importance” can relate to a range of actual definitions based on the analysis’s intent. Two general categories of “importance” have been proposed (Vivas et al., 2019). First, centrality indices reflecting network flow are critical nodes predicated on the classification of centrality based on the flow considered vital to a network (Opsahl et al., 2010). As an example, in financial network analysis, this is the amount of money flowing from firm to firm, where the out-strength of a node reflects direct spend or transfer of funds, and the in-strength represents receipt or acceptance of funds (Chan-Lau, 2018). This example results in the quantification of node importance in a minimum of two dimensions, dependency on money distribution (out) and the total holdings or receipts (in). Second, “importance” can be measured in terms of the coupling of nodes within a network. For example, in the modeling of pollination generalist species of plants, a tightly coupled sub-network of nodes increases the probability of cross-pollination among the subsets (Alvarez-Socorro et al., n.d.).

Leveraging Centrality and Community to Quantify Systemic Risk

As a novel approach to quantifying risk, vulnerabilities, and imbalances within the DIB, this research proposes that centrality and community measures provide critical insight into two macro forces threatening a supply chain. First, connectedness-based risk rankings quantify systemic risk. Second, community measures quantify fragility. A supplier can be both systemically risky and fragile. In this paper, the following arguments establish systemic risk, fragility, and imbalance: systemic risk directly relates to a supplier’s criticality within a supply chain network. A supplier with more influence carries a more significant negative impact on the overall network in the event of a disruption; it is, therefore, more systemically risky than a weakly-connected supplier. Fragility indicates vulnerability or the lack of supply chain network robustness (Perera et al., 2018). Larger communities with more outstanding overall systemic dependencies illustrate vulnerability within the supply chain network. Finally, imbalance represents disproportional levels of both risk and fragility for both commodities and suppliers.

In the remaining sections of the paper, Methodology details the network creation and structure and the applicability of specific centrality measures and community, thereby providing acquisition agencies with lower sub-tier visibility regardless of program or procurement authority. Results uses Aircraft NAICS as a use-case to apply network analysis; this analysis supports a key research objective of detecting, evaluating, and characterizing supply base threats capable of disrupting material availability. Lastly, Conclusions presents the conclusions of this research, with the intent that through further modeling and via a coupled methodical supplier development approach, a more resilient and responsive DIB can be developed.

Methodology

This section briefly describes the methods utilized to calculate centrality measures and assess modularity to support community identification.[1] Systemically critical suppliers exist as highly linked nodes throughout the network (central nodes), tightly coupled links within neighboring nodes (community nodes), or a state where the supplier is both central and tightly bound within a community.

Data Aggregation and Network Structure

This research is limited to unclassified, open-source acquisition data; no prime generated or propriety data is within the analysis. Therefore, the analysis is subject to contractor reporting accuracy for material spend disclosed per the Federal Funding Accountability and

[1] Underlying math foundations are provided as references.

Transparency Act of 2006 (FFATA). The FFATA requires that any federal contract, grant, loan, and other financial assistance awards of more than $25,000 are on a publicly accessible and searchable website. Data reporting is limited to first-tier suppliers; subcontract award information contains awardee, DUNS information, parent company information, award date, program usage, and material type. The provided illustrations show the type of data and views available from open-source government data for Army Missile Procurement (U.S. Department of the Treasury, Bureau of the Fiscal Service, 2021).

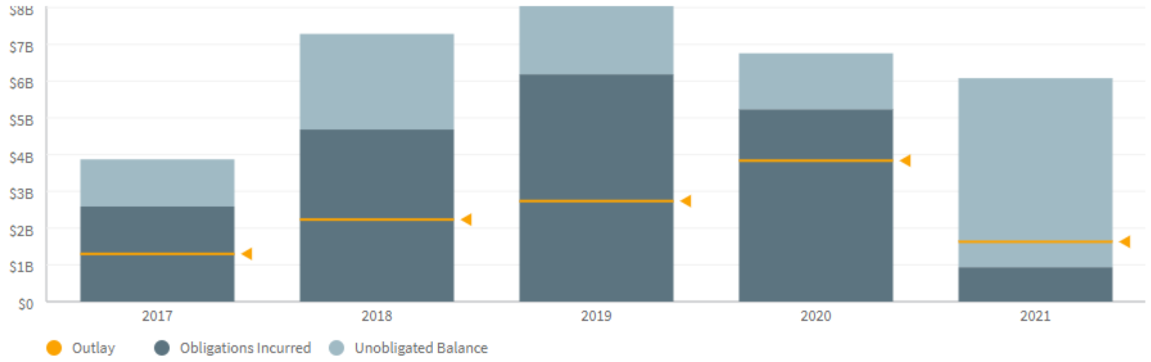


Figure 1. Spending Over Time (Fiscal Year [FY] 2017+ Army Missiles)

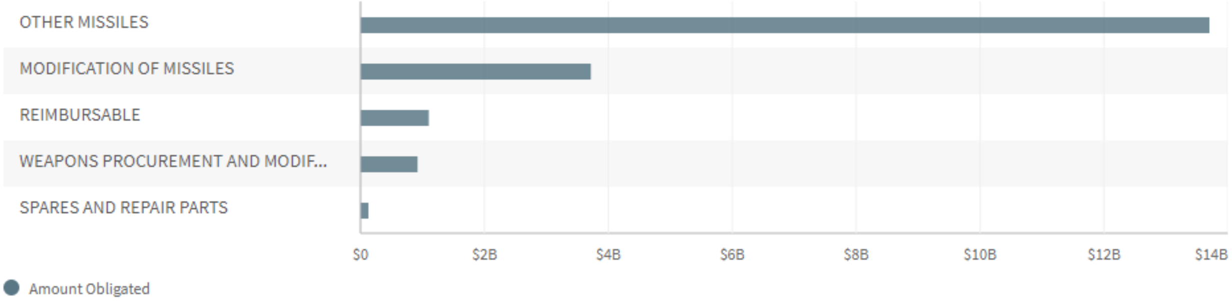


Figure 2. Spending by Category (FY2017+ Army Missiles)

Defense programs or NAICS commodities facilitate the analysis of relations between objects. Our vertices or nodes will represent the following organizations procuring agencies, prime contractors, and subcontractors (reference Figure 3). Edges will communicate both the existence of a relationship and a directed path or flow of acquisition dollars. Reference Figure 4 for an example of the visualization output.

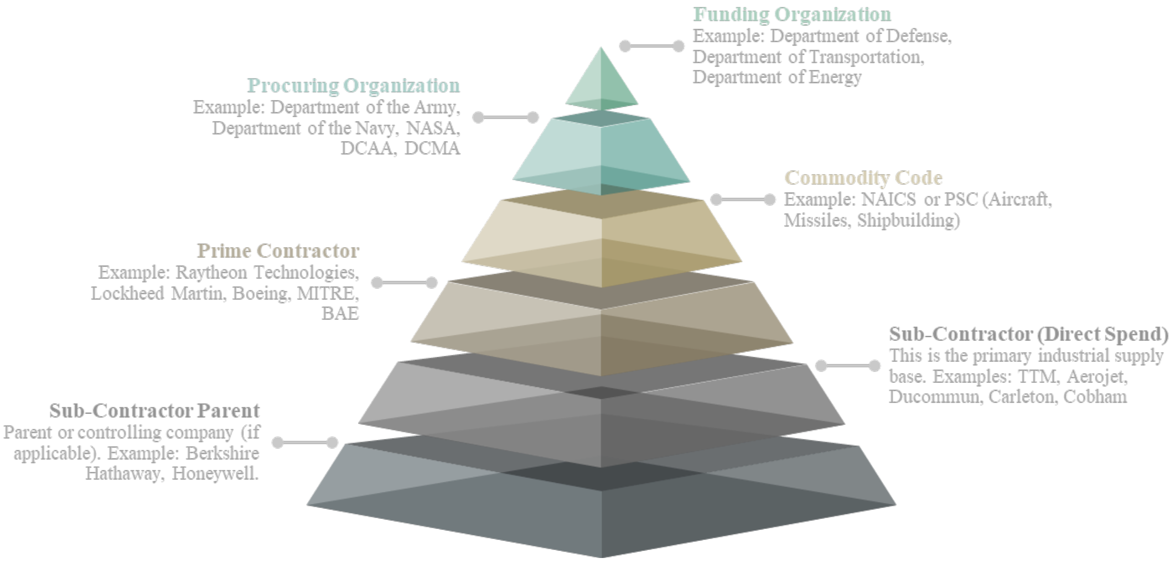

Funding Organization
Example: Department of Defense, Department of Transportation, Department of Energy
Procuring Organization
Example: Department of the Army, Department of the Navy, NASA, DCAA, DCMA
Commodity Code
Example: NAICS or PSC (Aircraft, Missiles, Shipbuilding)
Prime Contractor
Example: Raytheon Technologies, Lockheed Martin, Boeing, MITRE, BAE
Sub-Contractor (Direct Spend)
This is the primary industrial supply base. Examples: TTM, Aerojet, Ducommun, Carleton, Cobham
Sub-Contractor Parent
Parent or controlling company (if applicable). Example: Berkshire Hathaway, Honeywell.

Figure 3. Network Structure

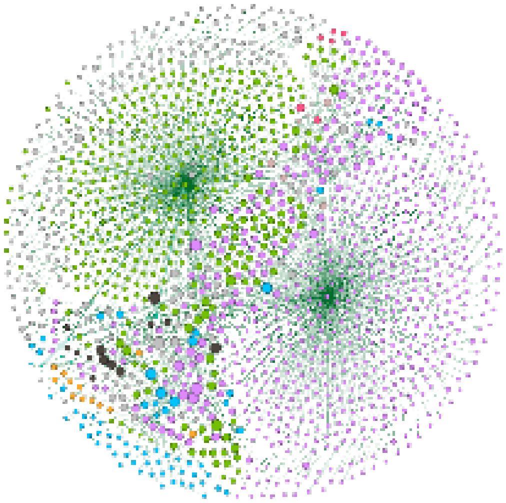


Figure 4. FY2019 Army Missile Procurement Visualization

Centrality (Node Level)

Centrality measures allow for identifying systemically critical suppliers in the supplier base; nodes reflect specific contractors and sub-contractors, node size reflects the centrality score, and color of the node reflects segregated communities' subsystems. Table 1 summarizes measures of centrality. Degree in this context is a local measure; the DIB financial network requires a global view of the supplier's connections. Alternative centrality measures are required to characterize systemically critical suppliers within the defense network correctly.

Table 1. Measures of Centrality

Item	Basis	Measure	DIB Applicability	Source
Degree	Importance score based on the number of links held by each node	Direct connections	In-degree and out-degree measures to better understand the flow of material	Perera et al., 2018
Betweenness	The number of times a node lies on the shortest path between other nodes	Network efficiency of flow	High betweenness indicates critical suppliers that are highly active within the network	Estrada et al., 2009
Closeness	Time required to spread information from a node to the other nodes in the network	Shortest paths between all nodes	Suppliers with high closeness centrality levels support mitigation of the impacts arising from bullwhip effect (Xu, et al., 2016)	Buechel & Buskens, 2013
EigenCentrality	Represents the relative strength or influence over other nodes in the network	Node influence	Quantifying the propagation of failure tied to disruption of a supplier	Ruhnau, 2000
PageRank	Similar to EigenCentrality, the assigned score reflects influence within the network, but PageRank also considers link direction and weight	Node Influence	The extent of failure propagated through a community of suppliers or across a commodity	Page, 1999

Communities (Network Level)

While centrality measures provide insight on systemically critical suppliers, the complexity and size of a macro-view of defense procurement requires an approach capable of accurately decomposing highly interconnected nodes into communities. Doing so supports the quantification of fragility in the multiple dimensions in which it can exist. The usage of community detection allows for analysis of tightly coupled suppliers, further facilitating quantification of likely common failure-mode points within the network. As the applicability of centrality measures, multiple methodologies of community detection are germane in network science. Table 2 shows some of these community measures.

Table 2. Measures of Community

Item	Basis	Measure	DIB Applicability	Source
Network Diameter	Edge count of the shortest path across the network	Complexity	Supports quantification of local community authority or the lack of authority across a commodity	Abd-El-Barr, 2009
Network Density	The level of interconnectivity between nodes	Connectivity	Higher density indicates a more robust supply chain	Bendle & Patterson, 2008
Clustering Coefficient	The level of coupling nodes demonstrated	Subsystem or neighborhoods	Assessing program, agency, or prime contractor supply chain dependencies	Brintrup et al., 2016
Modularity	The strength of the allocation of subsystems within a network	Subsystem or neighborhoods	Detecting community structure within an NAICS group	Fortunato & Barthelemy, 2007

Risk Association

Reference Figure 5 for an overview of the applied risk framework. This graph depicts relative community strength on the x-axis, where a higher assigned score represents a more substantial connected supplier. EigenCentrality scores compose the y-axis, indicating a supplier's strength or influence over other nodes in the network. Finally, the supplier node size represents a function of its relative community ranking and its overall authority within the network combined with the supplier's weighted indegree. Leveraging Centrality and Community to Quantify Systemic Risk proposed systemic risk, which is a risk to the overall supply chain network's efficiency or effectiveness, which could be determined using total supply-base influence measures. Two forms of risk are present: (1) the local criticality of a supplier, where subsequent supplier risk can be further defined using traditional defense industrial risk measures (reference Table 3) and (2) the systemic risk a node presents within its overall network or community.

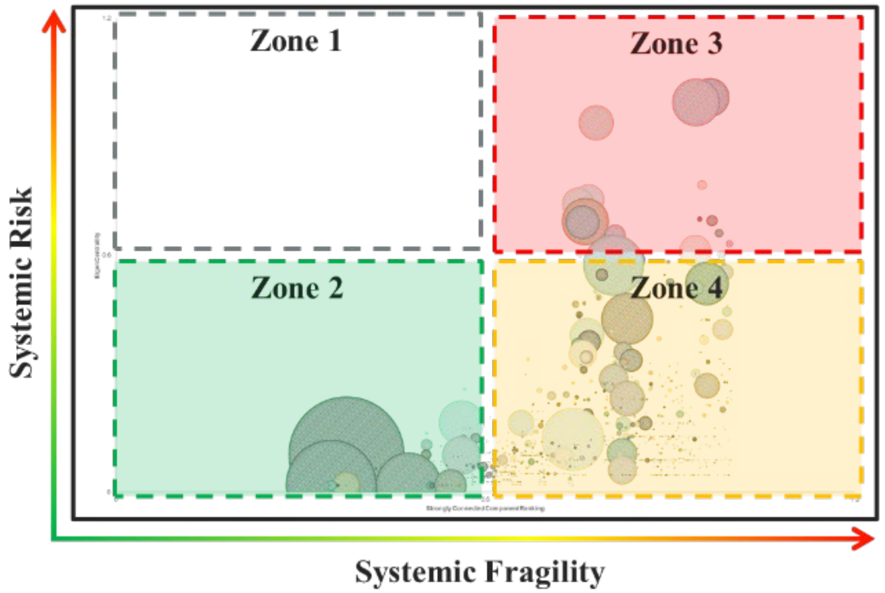


Figure 5. Mapping Risk to Centrality and Community

Four distinct zones form using this analysis technique. First is High-Systemic Risk and Low-Systemic Fragility; suppliers in this zone would carry considerable network influence but would have a lower strength of connection or community impact; this zone should be free of qualifying nodes, as a weakly connected supplier should not be supported with a high influence ranking. Second is Low-System Risk and Low Systemic-Fragility; suppliers in this zone would reflect both lower influence and community coupling, meaning they pose a low systemic threat; however, they carry considerable quantified local risk; as an example, prime contractors tend to appear here; they carry a disproportionally large total of spend with low in-strength. While these nodes are generally more central, nodes identified with more significant risk are more systemic. Third is High-Systemic Risk and High-Systemic Fragility; these suppliers are considered imbalanced; they are critical to the network from a community perspective; they also carry significant systemic risk. Additionally, their influence and in-degree can establish local risk. Fourth is Low-Systemic Risk and High-Systemic Fragility; these suppliers represent the absence of network robustness.

These measures are relative to the scope of the network analysis completed. For example, the Department of the Army spending analysis will result in a different set of identified risk, fragility, and imbalance than the same analysis focused on Department of the Navy spending. Moreover, the combination of both agencies will again shift quantification and output. Furthermore, analyzing modules or communities within an analysis will provide a different set of focus suppliers. This dynamic nature is critical for correctly identifying the specific threats for a cognizant program office or prime contractor and understanding the overlapping or shared risk.

Mapping Risk to Traditional Supply Chain Risk Areas

It is reasonable to leverage centrality and community measures against traditional risk areas. Table 3 provides GAO-identified risk areas threatening the DIB (GAO, 2018). By selecting node level measures with known supply chain network implications, further evaluation of systemically risky or fragile suppliers is achievable in terms of their local risk factors.

Table 3. Mapping Network Measure to Traditional Risk Areas

Traditional Risk Area (GAO)	Traditional Approaches	Concern	Pf Measures (Likelihood)	Cf Measures (Severity)
Financial Viability of Suppliers	Monitor – Monitor DUNS data as available	Shrinking DIB, inconsistent demand forecasting	DUNS Trend (6-month, 12-month) – Couple with community measures, the financial viability of the community	Highest betweenness levels within a community
Sole Source	Monitor – Quantitative at the program level	Single points of failure	Closeness centrality, ability to share demand	Highest Eigenvector measure within a network
Limited Production Capacity	Avoid - Qualitative, supplier RFPs	Inability to ramp quickly	Trend analysis supplier CAGR (increasing) Highest Eigenvector measure within a network; within a commodity	Highest Eigenvector measure within a network; within a commodity
Facility Damage by Disaster	Monitor - Quantitative concerning risk areas, qualitative regarding the impact	The failure mode of sole-source	Natural disaster probabilities/distributions	Supplier Geolocation – Number of programs/primes impacted. Highest Eigenvector measure within a network; within a commodity
Loss of Skill or Equipment	Accept – Difficult to quantify. Highly variable by program	Lack of manufacturing expertise and DIB investment funding	Trend analysis supplier CAGR (decreasing)	Highest Eigenvector measure within a network; within a commodity
Foreign Dependence	Mitigate - Quantitively at the prime level, qualitative at the subcontract level	Component dependencies external to the United States	DUNS Trend (6-month, 12-month) – Couple with community measures, the financial viability of the community, commercial market share	Parent DUNS, Highest Eigenvector measure within a network; within a commodity

As an example, reference Figure 6. This subset view of suppliers shows suppliers with the least betweenness centrality while still holding system risk. Closeness centrality is critical to the effectiveness of the supply chain in the presence of a degraded state or inaccurate demand planning (Perera et al., 2018); these detractors contribute to the "bull-whip" effect in supply chains (Xu et al., 2014). In our provided view, these are essentially critical suppliers within the network with limited or nonexistent closeness measures. They cannot share total demand and are therefore risk considerations for traditional concerns like sole sourcing, limited capacity, or loss of skill or equipment.

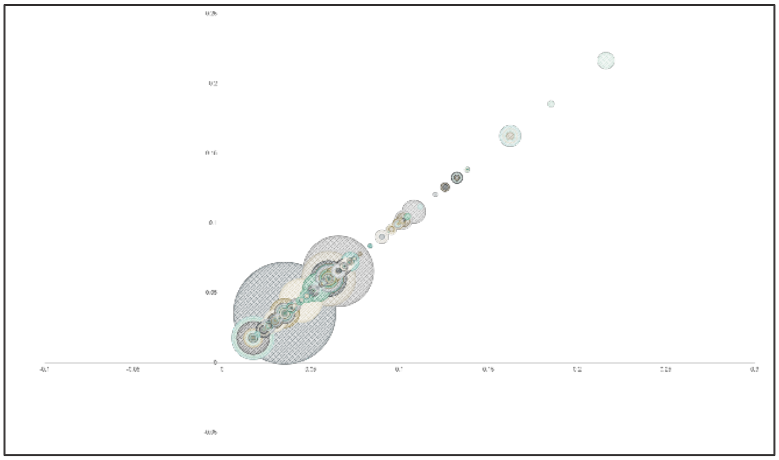


Figure 6. Network Measures Translated Into Sole-Source Risk

The following section provides the application of these processes. They show the use of the methods outlined as they relate to Aircraft manufacturing in FY2020. The output of this analysis will be the identification of systemic risk, fragility, and imbalance within the supply base.

Results

Application: FY2020 NAICS – Aircraft Manufacturing

This analysis evaluated roughly $25 billion in disclosed spend. Key prime contractors were BAE, Lockheed Martin, and Raytheon Technologies. NAICS analysis was limited to the following codes and their respective titles: Aircraft Manufacturing (336411), Aircraft Engine and Engine Part Manufacturing (336412), and Aircraft Parts and Auxiliary Equipment Manufacturing (336413). As a commodity, this represents deliverable items such as air vehicles, gas turbines, engine components, avionic subsystems, and engineering services. The primary procuring agencies are of the DoD, provided as follows in order of out-degree: Department of the Air Force, Department of the Navy, Defense Logistics Agency, Department of the Army, U.S. Special Operations Command, and the Defense Contract Management Agency.

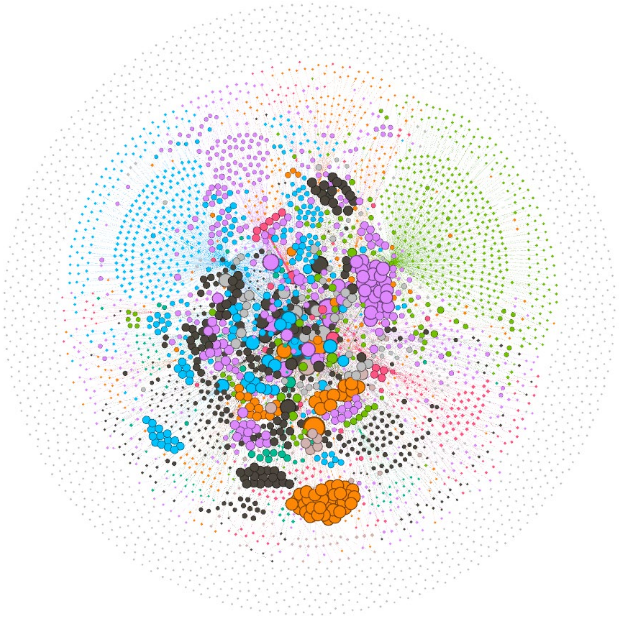


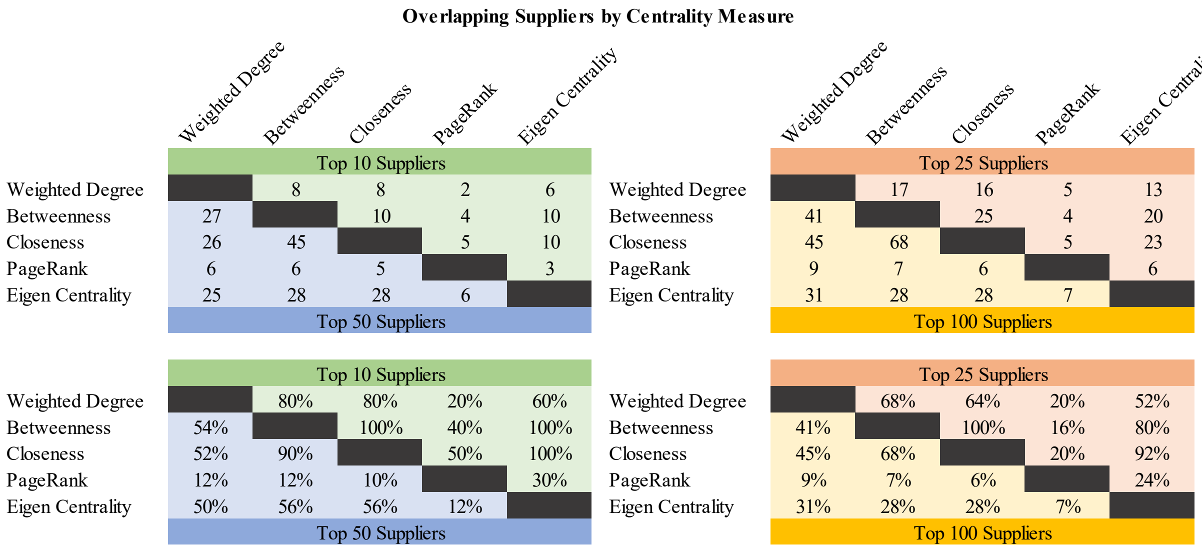
Figure 7. FY2020 NAICS Aircraft Supplier Network

Per Figure 7, the node's size reflects the network EigenCentrality score, conveying suppliers with network influence. The assigned node color indicates a subsystem within the network, and these are an output of the analysis of network modularity. Assigned modularity aligns with either a principal prime contractor, a specialized commodity provider with limited direct competitors (notable examples: sand castings, energetic materials, solid-state rocket motors), or a family of parent-company–owned sub-contract suppliers. As an example of wholly-owned subsidiaries driving communities, the suppliers United Technologies, Parker Hannifin, Aerojet, and L3 essentially build independent sub-tier mapping communities.

Aircraft Centrality Measures

Centrality for each supplier is quantified in four different measures: weighted degree, closeness, eigenvector centrality, and PageRank. These outputs provide the basis for fragility assessment; they inherently communicate the network's criticality based on a critical node's impact. The consequence in these terms is relative to the overall network versus a specific program or contractor; impact by a prime contractor can, however, directly map to an individual program. Table 4 summarizes the overlap of centrality-based network measures representing the systemic risk of sub-tier suppliers relative to the overall NAIC Aircraft supply base.

Table 4. Fragility Assessment Overlap (Centrality)



Overlapping Suppliers by Centrality Measure

	Weighted Degree	Betweenness	Closeness	PageRank	Eigen Centrality
	Top 10 Suppliers				
Weighted Degree	■	8	8	2	6
Betweenness	27	■	10	4	10
Closeness	26	45	■	5	10
PageRank	6	6	5	■	3
Eigen Centrality	25	28	28	6	■
	Top 50 Suppliers				

	Weighted Degree	Betweenness	Closeness	PageRank	Eigen Centrality
	Top 25 Suppliers				
Weighted Degree	■	17	16	5	13
Betweenness	41	■	25	4	20
Closeness	45	68	■	5	23
PageRank	9	7	6	■	6
Eigen Centrality	31	28	28	7	■
	Top 100 Suppliers				

	Weighted Degree	Betweenness	Closeness	PageRank	Eigen Centrality
	Top 10 Suppliers				
Weighted Degree	■	80%	80%	20%	60%
Betweenness	54%	■	100%	40%	100%
Closeness	52%	90%	■	50%	100%
PageRank	12%	12%	10%	■	30%
Eigen Centrality	50%	56%	56%	12%	■
	Top 50 Suppliers				

	Weighted Degree	Betweenness	Closeness	PageRank	Eigen Centrality
	Top 25 Suppliers				
Weighted Degree	■	68%	64%	20%	52%
Betweenness	41%	■	100%	16%	80%
Closeness	45%	68%	■	20%	92%
PageRank	9%	7%	6%	■	24%
Eigen Centrality	31%	28%	28%	7%	■
	Top 100 Suppliers				

When looking at the overlap of measures, suppliers' composition should draw attention to prime contractors' dependencies within the network. Table 5 shows the top 10 overlapping suppliers for this network.

Table 5. Top 10 Overlapping Suppliers (Aircraft NAIC FY2020)

SUPPLIER NAME	MODULARITY CLASS
UNITED TECHNOLOGIES CORPORATION	92
LEONARDO SPA	92
EATON CORPORATION PUBLIC LIMITED COMPANY	92
CURTISS-WRIGHT CORPORATION	92
BOEING COMPANY, THE	92
AMETEK INC.	92
L3HARRIS TECHNOLOGIES, INC.	93
Transdigm Group Incorporated	93
HEICO CORPORATION	93
NORTHROP GRUMMAN CORPORATION	122

The presence of crucial prime contractors results from their weighted degree per the analysis provided in Table 4. In this example, suppliers like United Technology, Boeing, and Northrop Grumman are sub-contracts to prime spending. Their complete failure concerning the network (e.g., bankruptcy) is improbable. Overlapping firms carry the highest overall fragility or concern. Their respective modularity classifications convey the interdependencies that exist. These suppliers are not only critical to the performance of the supply chain network but are also highly dependent on each other. Traditional monitoring methods and assignment of fragility, criticality, or risk based on total monetary spend, whether it be by program or supplier, are insufficient to characterize total industry fragility.

Expanding on the measurement intent outlay provided within the Methodology section, consider the following: The discernible differences in identified suppliers indicate that different centrality measures indicate that dimensions of fragility exist for supply chain networks by lumping measures together or looking myopically at total spending hides suppliers with considerable network influence. Table 6 provides a conceptual approach to matching dimensional fragility measures with traditional supply base risk measures.

Table 6. Centrality Based Fragility Mapped to Systemic Risk Drivers

Measure	Fragility Dimension	Systemic Risk Drivers
Weighted Degree	Primarily parent companies, or direct subcontract award to major prime contractors. The network is dependent on forecasted demand	• Demand Uncertainty • Budget Uncertainty • Natural Disaster or Malicious Attack
Betweenness	Composed of "bridge suppliers," this model moves to the first tier of the prime contractor supplier spend. As an effect, these are primarily parent suppliers or familiar sources of supply for generic material (electronic components, fasteners)	• Foreign Dependence • Single Sources of Supply
Closeness	Relatively high overlap of closeness and weighted degree indicates that the network's agility or speed depends on large tier suppliers. Respective capabilities and capacities should facilitate shorter paths through the network.	• Limited production capacity • Foreign Dependence • Natural Disaster or Malicious Attack
PageRank	The PageRank algorithm consistently highlights influential suppliers outside of the top spend.	• Obsolete Items • Financial Viability of Suppliers • Sole sourcing • Loss of skill or equipment
EigenCentrality	They are highly coupled or connected suppliers within the network; their dependencies cross over programs, procuring agencies, and even commodities.	• Limited production capacity • Foreign Dependence • Loss of skill or equipment • Financial viability • Sole source • Natural Disaster or Malicious Attack

Aircraft Supply Chain Network – Systemic Risk

The suppliers listed in Table 7 carry the highest systemic risk within this commodity code. The EigenCentrality measure dictates the supplier (displayed in Figure 8). There is a range of technical capability provisions listed, and this suggests critical suppliers across a broad spectrum of provided solutions. The influence of these suppliers propagates through the supply chain network. Their disruption impacts parent companies, prime contractors, and coupled procurement agencies. It is important to note that these suppliers share community measures; Aircraft Supply Chair Network – Systemic Module Risk describes the impacts to systemic risk at a community level.

Table 7. Top 10 Systemic Risk Suppliers

SUPPLIER NAME	PROVISION
GOODRICH CORPORATION	Lighting Systems, Actuation, and Control
HAMILTON CORPORATION	Propulsion Systems, Flight Control Systems
COBHAM INC.	Antenna, Electronic Subsystem, RAD-Hard
AMI INDUSTRIES, INC.	Emergency evacuation systems, Seating systems, Life rafts
B/E AEROSPACE, INC.	Structures
INTERTRADE LIMITED	Recertified airframe and engine parts
EXOTIC METALS FORMING LLC	Engine ducting and exhausts
L3HARRIS TECHNOLOGIES, INC.	R.F. equipment, Data Link Communication
WESCAM INC	Air Surveillance and Reconnaissance
CHELTON AVIONICS, INC.	Antenna systems, avionics systems, electronics systems

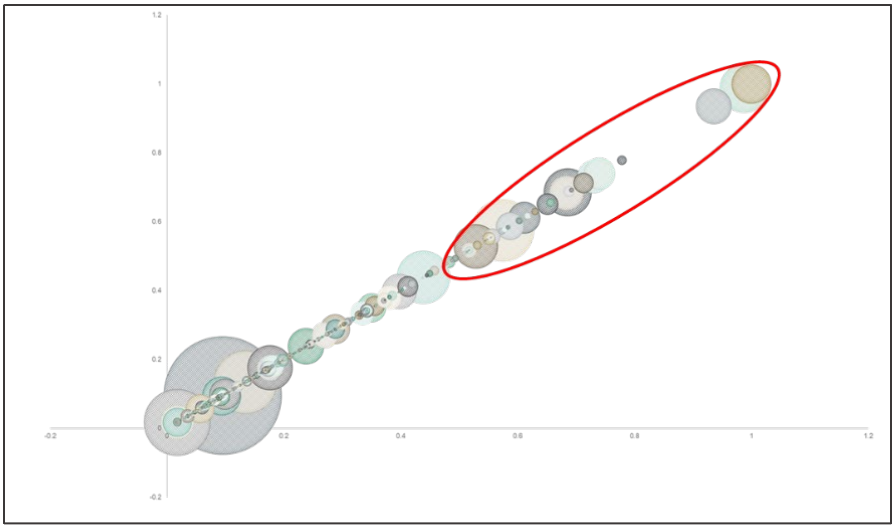


Figure 8. Aircraft Systemic Risk Visualization

Aircraft Supply Chain Network – Systemic Module Risk

A crucial module or communities that formed within the network centered around United Technologies Corporation (UTC). UTC is a parent company within this analysis; the basis for this community is derived from the material acquisition across NAICS either directly to UTC or one of their wholly-owned subsidiaries. While the complete list of suppliers will not result in a complete module composed of UTC subsidiaries, Table 8 provides a list of the top 10 systemically risky suppliers within the module. This analysis provides a supply chain manager insight into critical dependencies within a community. More notably, this analysis supports further risk characterization based on the supplier's authority and valuation (size of the node); reference Figure 9.

Table 8. Systemic Risk - Module Analysis

SUPPLIER NAME	PARENT COMPANY
HAMILTON SUNDSTRAND CORPORATION	UNITED TECHNOLOGIES CORPORATION
GOODRICH CORPORATION	UNITED TECHNOLOGIES CORPORATION
Rockwell Collins, Inc.	UNITED TECHNOLOGIES CORPORATION
AMI INDUSTRIES, INC.	UNITED TECHNOLOGIES CORPORATION
B/E AEROSPACE, INC.	UNITED TECHNOLOGIES CORPORATION
INTERTRADE LIMITED	UNITED TECHNOLOGIES CORPORATION
GOODRICH ACTUATION SYSTEMS SAS	UNITED TECHNOLOGIES CORPORATION
ROSEMOUNT AEROSPACE INC.	UNITED TECHNOLOGIES CORPORATION
J. A. REINHARDT & CO., INC.	UNITED TECHNOLOGIES CORPORATION
GOODRICH LIGHTING SYSTEMS, INC.	UNITED TECHNOLOGIES CORPORATION
GOODRICH ACTUATION SYSTEMS LTD	UNITED TECHNOLOGIES CORPORATION

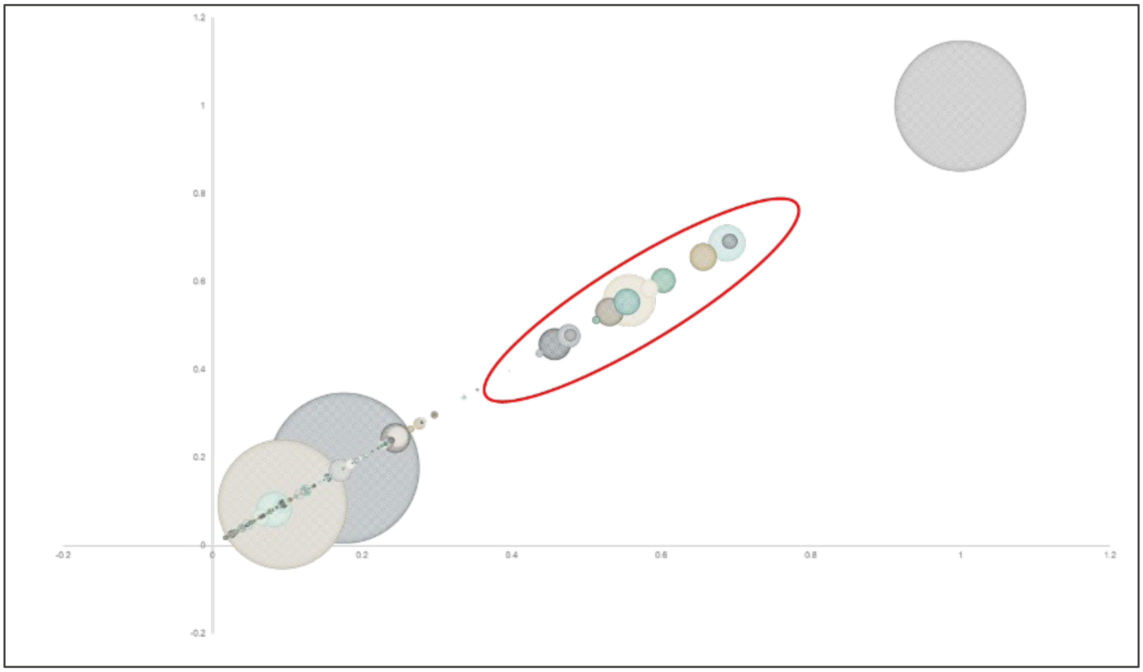


Figure 9. Systemic Risk - Module Analysis

Aircraft Supply Chain Network – Systemic Fragility

Table 9 lists top identified suppliers as a function of their authority and relative component strength measure. These represent weak points in the supply chain network. They are network vulnerabilities with the general implication that there is no ready-made set of alternative sourcing options.

Table 9 – Top 10 Systemic Fragility Suppliers

SUPPLIER NAME	PROVISION
ACME EMBEDDED SOLUTIONS	Ruggedized Computing Systems
SIERRA ALLOYS COMPANY	Titanium Manufacturing
PERILLO INDUSTRIES, INC.	Power Subsystems
FIBREFORM ELECTRONICS, INC.	Precision Machining
TORAY ADVANCED COMPOSITES ADS, LLC	Composite Materials
S&L AEROSPACE METALS, LLC	Structural Machining
RIVERSIDE MACHINE & ENGINEERING, INC.	Precision Machining
MICROWAVE DEVELOPMENT LABORATORIES, INC.	Waveguide Components
ADVANCED CONVERSION TECHNOLOGY, INC.	Power Subsystems
BOEDEKER PLASTICS, INC.	Molded Plastics

Aircraft Supply Chain Network – Imbalance

Given the massive nature of this supply chain network, narrowing systemic risk and fragility to each category's top 10 drivers is less than ideal for taking a pragmatic approach to improving the base's robustness. The concept of imbalance introduced in the Literature Review can narrow systemic risk and fragility into network-specific threats, as shown in Figure 10.

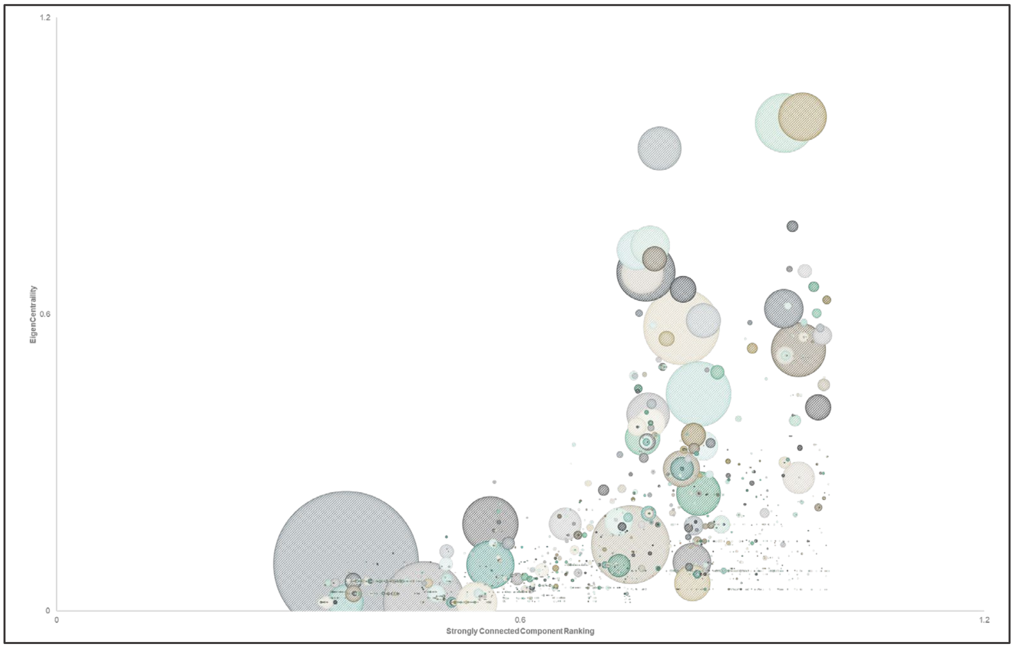


Figure 10. Aircraft NAICS - Imbalance Assessment

In Aircraft manufacturing, the following sub commodities are systemically risky and fragile: titanium manufacturing and forging, engine component manufacturing, structures, and precision machining. The suppliers providing this material share similar network influence measures and are primarily shared sources of supply regardless of the prime contractor, consequently resulting in a disproportional (imbalanced) amount of total spend distribution and, consequently, network criticality assignment. This analysis augmented with targeted supplier development efforts would both highlight and make mitigation activities actionable. These are critical points within the supply base that could be augmented with direct investment in capabilities, training, and long-term demand stabilization or additional suppliers developed to build redundancy in the overall network.

Conclusions

We have presented a detailed approach for leveraging centrality and community measures to quantify systemic risk, vulnerability, and imbalance in defense supply chain networks. This approach evaluates defense procurement supply-base resiliency by commodity, program execution office, or overarching defense procurement agency. As a result, the following three objectives and their conclusions are as follows: First, systemic risk is quantified using centrality measures to identify the most critical nodes within the network. A supplier with more influence carries a more significant negative impact on the overall network in the event of disruption and is, therefore, more systemically risky. Second, DIB fragility is quantified using community measures; facilitating identification of communities with more significant overall systemic dependencies illustrates vulnerability within the supply chain network. Third, imbalance represents disproportional levels of both risk and fragility in both specific commodities and suppliers.

To illustrate the application of these concepts, an FY2020 view of Aircraft manufacturing was provided. This analysis addressed 80,000+ records of subcontract procurement for material ranging from fasteners to avionic subsystems. This visualization facilitated the identification of suppliers in terms of systemic risk and fragility in the following technical areas: power subsystems, structures, forgings, microwave components, and electronic components. Furthermore, a novel approach to quantifying traditional risk measures using centrality and community detection was proposed, highlighting sole source risks within a network.

By leveraging network analysis principles and practices, we have demonstrated how application within the DIB can differentiate supplier criticality. Future work will refine supplier risk measures and integrate trend analysis to quantify industry contraction or expansion by commodity. Additionally, a dynamic version of this modeling application is in work, supporting modeling and simulation of the DIB to quantify the consequences of systemic failures further.

References

Abd-El-Barr, M. (2009). Review: Topological network design: A survey. *Journal of Network and Computer Applications*, *32*(3), 501–509. https://sciencedirect.com/science/article/pii/s108480450800101x

Alvarez-Socorro, A. J., Herrera-Almarza, G. C., & González-Díaz, L. A. (n.d.). Eigencentrality based on dissimilarity measures reveals central nodes in complex networks. *Scientific Reports, 5*, 17095. http://www.nature.com/articles/srep17095

Asbjørnslett, B. (2008). Assessing the vulnerability of supply chains. In G. A. Zsidisin and B. Ritchie (Eds.), *Supply chain risk: A handbook of assessment, management & performance* (pp. 15–33). Springer.

Aviles, L., & Sleeper, S. (2016). *Identifying and mitigating the impact of the Budget Control Act on high-risk sectors and tiers of the defense industrial base: Assessment approach to industrial base risks*. https://apps.dtic.mil/sti/citations/AD1016751

Bendle, L. J., & Patterson, I. (2008). Network density, centrality, and communication in a serious leisure social world. *Annals of Leisure Research, 11*, 1–19. http://tandfonline.com/doi/pdf/10.1080/11745398.2008.9686783

Blackhurst, J. V., Scheibe, K. P., & Johnson, D. J. (2008). Supplier risk assessment and monitoring. *International Journal of Physical Distribution & Logistics Management*, 143–165.

Bonacich, P. (1987). Power and centrality: A family of measures. *American Journal of Sociology*, *92*(5), 1170–1182.

Brintrup, A., Ledwoch, A., & Barros, J. (2016). Topological robustness of the global automotive industry. *Logistics Research*, *9*(1), 1–17. https://link.springer.com/article/10.1007/s12159-015-0128-1

Buechel, B., & Buskens, V. (2013). The dynamics of closeness and betweenness. *Journal of Mathematical Sociology*, *37*(3), 159–191. https://ideas.repec.org/p/bie/wpaper/398.html

Chan-Lau, J. A. (2018). Systemic centrality and systemic communities in financial networks. *Quantitative Finance and Economics*, 468–496.

Chopra, S., & Meindl, P. (2009). *Supply chain management* (4th ed.). Prentice-Hall.

DoD. (2008). *Defense Critical Infrastructure Program (DCIP): DoD mission-based Critical Asset Identification Process (CAIP)* (DoDM 3020.45-V1). Office of the Under Secretary of Defense for Policy.

DoD. (2018). *Assessing and strengthening the manufacturing and defense industrial base and supply chain resiliency of the United States.* Office of the Under Secretary of Defense.

Estrada, E., Higham, D. J., & Hatano, N. (2009). Communicability betweenness in complex networks. *Physica A: Statistical Mechanics and Its Applications*, *388*(5), 764–774. https://www.sciencedirect.com/science/article/abs/pii/S0378437108009473

Finch, P. (2004). Supply chain risk management. *Supply Chain Management*, *9*(2), 183–196. https://emerald.com/insight/content/doi/10.1108/13598540410527079/full/html

Fortunato, S., & Barthelemy, M. (2007). Resolution limit in community detection. *Proceedings of the National Academy of Sciences of the United States of America*, *104*(1), 36–41. http://www.pnas.org/content/104/1/36.abstract

GAO. (2017). *Defense supply chain: DOD needs complete information on single sources of supply to proactively manage the risks* (GAO-17-768).

GAO. (2018). *Integrating existing supplier data and addressing workforce challenges could improve risk analysis* (GAO-18-435).

González, A. M., Dalsgaard, B., & Olesen, J. M. (2010). Centrality measures and the importance of generalist species in pollination networks. *Ecological Complexity*, *7*(1), 36–43. https://sciencedirect.com/science/article/pii/s1476945x09000294

Hallikas, J. (2004). Risk management processes in supplier networks. *International Journal of Production Economics*, *90*(1), 47–58.

Hubbard, D. (2009). *The failure of risk management: Why it's broken and how to fix it.* John Wiley & Sons.

Lambert, D. M., & Cooper, M. C. (2000). Issues in supply chain management. *Industrial Marketing Management*, *29*(1), 65–83. https://sciencedirect.com/science/article/abs/pii/s0019850199001133

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management*, *38*(3), 192–223.

Meyer, M., Brintrup, A., & Windt, K. (2014). Linking product and machine network structure using nested pattern analysis. *Procedia CIRP*, *17*, 278–283. https://sciencedirect.com/science/article/pii/s2212827114003412

Newman, M. E. (2008). The mathematics of networks. In *The new Palgrave dictionary of economics* (2nd ed.), 3-4. http://www-personal.umich.edu/~mejn/papers/palgrave.pdf

Nishat, F. M., Banwet, D. K., & Shankar, R. (2006). Mapping supply chains on risk and customer sensitivity dimensions. *Industrial Management and Data Systems*, *106*(6), 878–895.

Opsahl, T., Agneessens, F., & Skvoretz, J. (2010). Node centrality in weighted networks: Generalizing degree and shortest paths. *Social Networks*, *32*(3), 245–251. http://toreopsahl.com/2010/04/21/article-node-centrality-in-weighted-networks-generalizing-degree-and-shortest-paths/

Outdot, J. M. (2010). *Journal of Public Policy*, *30*(2), 201–218.

Page, L., Brin, S., Motwani, R., & Winograd, T. (1999). *The PageRank citation ranking: Bringing order to the web*. Stanford University InfoLab Publication Server. http://ilpubs.stanford.edu:8090/422/1/1999-66.pdf

Perera, S., Bell, M. G., & Bliemer, M. C. (2018). *Network science approach to modelling emergence and topological robustness of supply networks: A review and perspective*. arXiv: Physics and Society. https://arxiv.org/abs/1803.09913

Rao, S., & Goldsby, T. J. (2009). Supply chain risks: A review and typology. *The International Journal of Logistics Management*, *20*(1), 97–112.

Ruhnau, B. (2000). Eigenvector-centrality—A node-centrality? *Social Networks*, *22*(4), 357–365. https://sciencedirect.com/science/article/pii/s0378873300000319

Schafer, M. H. (2011). Health and network centrality in a continuing care retirement community. *Journals of Gerontology: Series B, Psychological Sciences and Social Sciences*, *66B*(6), 795–803. https://academic.oup.com/psychsocgerontology/article/66b/6/795/593397

Sinha, P. R., Whitman, L. E., & Malzahn, D. E. (2004). Methodology to mitigate supplier risk in an aerospace supply chain. *Supply Chain Management*, *9*(2), 154–168. https://emerald.com/insight/content/doi/10.1108/13598540410527051/full/html

U.S. Department of the Treasury, Bureau of the Fiscal Service. (2021). *USAspending.gov*. https://www.usaspending.gov/

Vivas, R. d., Sant'Anna, A. M., Esquerre, K., & Freires, F. G. (2019). Integrated method combining analytical and mathematical models for the evaluation and optimization of sustainable supply chains: A Brazilian case study. *Computers & Industrial Engineering*, 105670. https://sciencedirect.com/science/article/pii/s0360835219300476

Wang, W., & Street, W. N. (2015). Modeling influence diffusion to uncover influence centrality and community structure in social networks. *Social Network Analysis and Mining*, *5*(1), 15. https://link.springer.com/article/10.1007/s13278-015-0254-4

Xu, M., Wang, X., & Zhao, L. (2014). Predicted supply chain resilience based on structural evolution against random supply disruptions. *International Journal of Systems Science: Operations & Logistics*, *1*(2), 105–117.

Xu, N-R., Liu, J-B., Li, D-X., & Wang, J. (2016). Research on evolutionary mechanism of agile supply chain network via complex network theory. *Mathematical Problems in Engineering*, 1, 1–9.

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net