WHITE PAPER

# Network Analytics and Digital Twin:
## Identifying and mitigating risks in defence supply chain and logistics.

Authors: Singupuram, Vamsi; Agrawal, Shreya; Guha, Saurabh

# Contents

For more information about our solutions, please visit
www.tcgdigital.com

*Abstract: Digital twin is at the heart of Industry 4.0 solutions for Supply Chain. Equipped with an intricately mapped supply chain network, a digital twin can enable organizations to simulate possible scenarios and identify possible choke points as well as predict and respond to shocks in real-time. This white paper starts with an introduction to familiarize readers with the kinds of supply chain shocks that an organization must prepare for. It then proposes a recursive approach to map a supply chain network and provides a framework for defining the components of the network, before describing a digital twin that can effectively harness the potential of the mapped supply chain network. Finally, it touches upon the stress testing methods that can be used to predict shocks to unlock value from the digital twin.*

# 1. Introduction

The last few decades have led to a meteoric rise in globalisation, supported by rapid advances in technology, and industrialisation. Global supply chains have followed suit, and have become extremely complex, connected and process-driven. The supply chain in the defense sector is no exception to this. Any vulnerability or shock has the ability to upend supply chains to varying degrees. These shocks can be as minor as a localised cyberattack, and can also be a major pandemic. The phenomenon of propagation of shock to various stakeholders upstream and downstream of the supply chain makes it crucial to understand the global supply chain with an eagle's eye view first and then focus on the specific differences that necessitate differential treatment for the defense supply chain in particular.

| Unanticipated Catastrophes | Foreseeable Catastrophes |
|---|---|
| Costs running into 10s of trillions of $s<br>Less lead time<br>Eg. systemic cyberattack, acute climate event, solar storm, meteoroid strike<br>Very unlikely/hasn't occurred yet | Costs running into 10s of trillions of $s<br>More lead time<br>Eg. pandemic, financial crisis, global military conflict<br>Less frequent |
| **Unanticipated Catastrophes**<br>Costs running into 100s of billions of $s<br>Less lead time<br>Eg. terrorism, theft, common cyberattack<br>More frequent | **Foreseeable Disruptions**<br>Costs running into 100s of billions of $s<br>More lead time<br>Eg. regulations, local military conflict<br>Somewhat frequent |

*Table 1: Categorization of shocks*

Usually, short disruptions (1-2 weeks) occur every 2 years, while a long disruption occurs every 5 years on an average. Exposure to shocks can be wide ranging across sectors and value chains. The overall shock exposure is often the highest for the communication equipment industry, albeit in a pandemic scenario, the aerospace industry is usually one of the most affected. During trade disputes, it is the semiconductors and communication equipment industries that are impacted the most. Also, in the event of a large cyberattack, the aerospace industry faces the maximum impact.

For more information about our solutions, please visit
www.tcgdigital.com

However, the financial implications are only a fraction of the net impact of a disruption in the defense supply chain as lives of the personnel, national security and interests are also on the line. It is thus of paramount importance to understand the contribution of various actors towards the readiness, availability, sustainability and preparedness and thereby monitor "fragility and criticality" of the supply chain at various levels to assess the risk exposure so as to act towards mitigating that risk through redundancies and policy changes. Essentially, while the core metric of a commercial supply chain is its efficiency, for a defense supply chain it is its effectiveness.

The covid-19 pandemic is a lesson for the detrimental effect of complacency in risk measurement and management in global supply chain systems. Nevertheless, the pandemic has exposed a wide range of vulnerabilities and bottlenecks, which have a lot of potential to be harnessed for creating robust models to support, predict and mitigate the consequences of disruptions and catastrophes on modern supply chains.

## 2. Mapping the Supply Chain Network

A supply chain network can be understood as a combination of nodes with capacity and capability, connected with lanes to facilitate movement of products between them. Here nodes represent the system components, such as firms, suppliers, facilities, and customers among many others. To create a comprehensive view of the supply chain, it is important to map all these nodes at a detailed sub tier level and identify hidden relationships which invite vulnerabilities.

To build such a network a recursive approach is best suited.

- Identify the high priority items and then iteratively going down to their component suppliers/ dependencies
- Start with the available data at the first layer of suppliers, i.e. the data about those suppliers who are directly in contact with the organization.
- Then, to go further in the network, the suppliers at the first layer will be surveyed to obtain the data to model the next layer and so on.
- At every such move from one layer to the next, the missing data and data regarding alternatives is sourced from publicly available data sets and other historical data available to the organization or the current layer of the network.

## 3. Defining Network Properties & Risk Parameters

Once the relationships between the nodes are established, it is important to define metrics which will help us investigate the characteristics of the network.

| Node Level Properties | Network Level Properties | Link Level Properties |
|---|---|---|
| • Centrality<br>• Clustering<br>• Embeddedness | • Network density<br>• Network centralization<br>• Clustering | • Flow type<br>• Multiplexity (multiple ties) tie strength |

*Table 2: Some of the most commonly used metrics in network analytics*

For more information about our  solutions, please visit
www.tcgdigital.com

Fragility and Criticality is currently the assessment methodology used by the department of defense for risk assessment. "Fragility" and "criticality" are roughly analogous to the traditional risk factors of probability and consequence. Fragility characteristics are those that make a specific product or service likely to be disrupted. Criticality characteristics are those that make a product or service difficult to replace.

The fragility-and-criticality methodology is currently applied for capturing the health and assessing the risk exposure of particular defense sectors, subsectors and direct suppliers. However, if more granular supply chain data were available, the methodology could be adapted to measure fragility and criticality at that greater level of detail at each node in the network.

| Criticality of the node | | | Fragility of the node | | |
|---|---|---|---|---|---|
| **Product** | **Costs** | **Preparedness** | **Geo-Location** | **Reliability** | **Agility** |
| Qualitative/Quantitative importance of the product | Cost and feasibility | Mitigation strategies for this supplier-product combination | Supplier site location | Variability in performance | Supplier risk assessment |
| Annual volume<br><br>- Inventory information (days of supply) | - Expediting components from other locations- the uniqueness of the components<br><br>- Additional resources (overtime, shifts, alternate capacity) | - Alternate suppliers<br><br>- Excess inventory | - Using the location of each site-type and organization-type node to approximately specify the relationship of the supplier country | - Lead times from supplier site<br><br>- Time to recovery (TTR) and Time to survive (TTS) | - Financial Stability<br><br>- Single source vs multi-source production<br><br>- Upstream material availability at alternate vendors |

*Table 3: Parameters used to assess risk at each node*

# 4. Real time risk monitoring with Digital Twins

A digital twin can be seen as a part of a control tower which is the central point for enhanced visibility and decision making. It would generally includes the following

- Data module that connects to data silos and ensures that the model's variables are updated and relevant
- Visualization module that includes data analysis, presentation and insights
- Current state/History module to check if service levels are being met and to perform historical analysis
- Decision support/Forecast module to perform scenario analysis, avoiding potential problems, and developing action plans
- Task and case management module for tracking and implementing an action plan

For more information about our solutions, please visit
www.tcgdigital.com

The supply chain network map can now be visualised in its operational form using a digital twin by utilising real time data on demand, supply, inventory levels etc.

## Risk Quantification

We can also quantify different types of risks at each node and arc based on network properties and risk related variables as defined above. Depending on the provided supply chain network, inputs from expert personnel might also be required for defining risk quantification of some variables. Once risk levels have been quantified/calculated, factors can be grouped and unified risk indexes can be calculated using techniques like principal component analysis.

These unified risk indexes, which represent the cumulative impact of a multitude of factors, provide a simplified and decluttered view of the risk landscape. The risk levels can be monitored in real time with alerts configured at predefined levels. Decision makers can utilize this information on risk build-up to take corrective action in time to mitigate the risk.

| | In-Degree Centrality | Out-Degree Centrality | Closeness Centrality | Eccentricity |
|---|---|---|---|---|
| Description of network metric | Number of incoming links represents the number of materials (e.g., elements, materials, parts, or components) required by a supplier to obtain the product | Number of outgoing links represent: (1) the number of downstream nodes (in cases where the node does not produce the final product) and (2) number of production sites of a supplier | The average steps from the node under investigation to any other node in the network. Indicator of transformation steps and contractual relationships | Indicates transformation steps only. |
| Description of network metric | Higher in-degree centrality translates into higher product complexity. | Higher connectivity translates into higher producer diversity or multiple downstream uses. | More transformation steps increase the likelihood for distortion. Each contractual relationship adds a layer of information or monetary flows. | More steps translate into increased likelihood for distortion of flows in the supply chain. |

*Table 4: A high level view of how centrality impacts risk*

In table-4, a transformation step can indicate either a physical transformation of material to product, packaging, aggregation or distribution (for eg. in a relief aid project, the final node is the node where

## 5.  Stress testing SCNs with Simulation

It is rare for commercial industrial supply chains to experience sudden increases in demand of 200-400%. The requirement is, however, relevant in the defense industry since its participants have to maintain their readiness to meet increased demands in case of wars and conflicts. Indeed, upside production flexibility, that is, the capability of unplanned sustained increase in production to support a two-major-theatre war scenario has been recommended as a key performance indicator for defense industry

For more information about our solutions, please visit
www.tcgdigital.com

Simulations provide the capability to evaluate the performance of any system under varied operating conditions, configuration, policies and procedures. Given the complexity of defence supply chains, with numerous nodes interacting amongst each other in multiple ways and across geography, it is an ideal tool to identify and demonstrate the behavior of the supply chain under stress and evaluate strategies to meet the defined goals.

The goals of the simulation are defined as:
- Evaluation of the supply chain network for meeting defined demand scenarios including those that highly stress the supply chain.
- Identification of areas that potentially limit the ability of the supply chain.
- Development and validation of supply chain configuration enhancements that allow it to meet the requirements.

## Monte Carlo Simulation

We now use the Monte Carlo simulation to create an operational profile for every node or arc in the supply chain. Monte Carlo methods are a class of simulation algorithms which work on the principle of using random sampling of historical data to replicate systems where the probability of varying outcomes cannot be determined because of random variable interference. It takes the variable that has uncertainty and assigns it a random value using statistical distribution of the historical data. The model is then run and a result is provided. This process is repeated again and again while assigning the variable in question with many different values. Once the simulation is complete, the results are averaged together to provide an estimate.
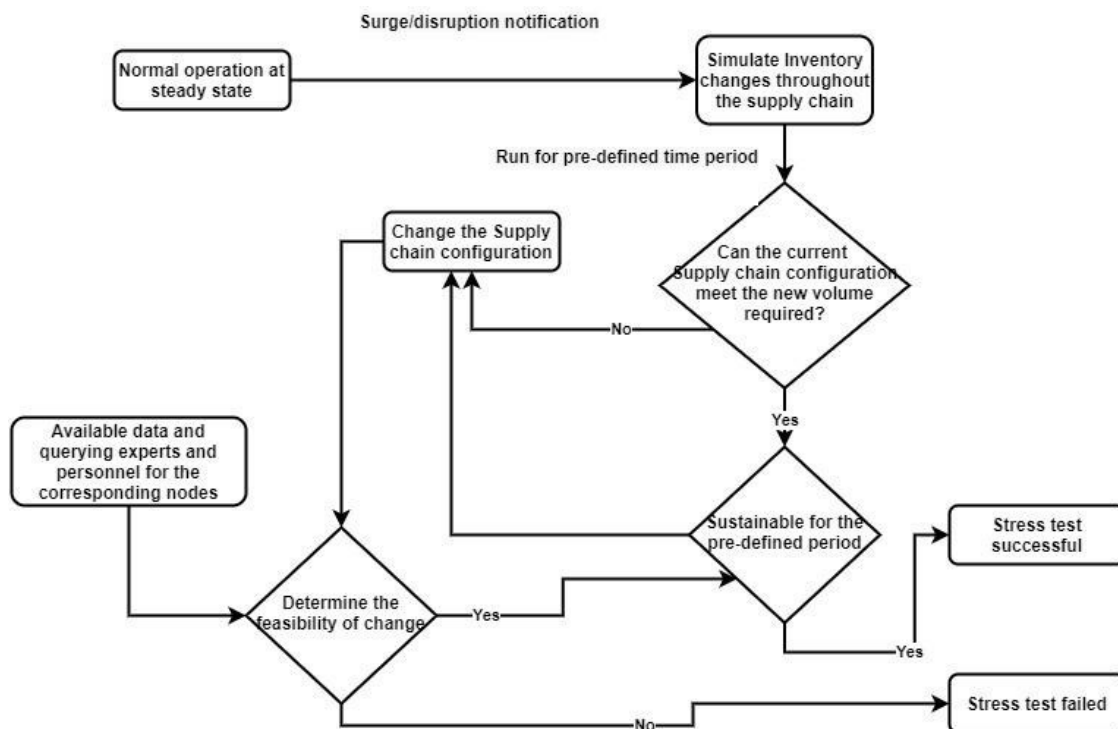


*Fig 2: Schematic design of the simulation architecture*

We use the historical data of demand, supply, inventory levels etc combined with inputs from external nodes to create statistical distributions which describe local operational envelopes of each node and arc.

For more information about our solutions, please visit
www.tcgdigital.com

These local simulations are then allowed to interact with each other; the rules and paths of these interactions are defined using the supply chain network map. As these simulations interact with each other and affect each other, the complex interdependencies of the network emerge. The method also provides us control knobs in the shape of initial conditions, which we can turn to create a wide range of operational scenarios and inventory changes across the network.

Broadly, we can classify the simulations we can model into 4 possible scenarios:
- Normal operation
- Localized disruptions (most likely scenario) - reallocation and relocation of resources
- Catastrophe (worst case scenario) - production from suppliers from every layer will go down due to the financial/operational implications of the disruption
- Recovery (best case scenario) - some suppliers will shut down and
  - Expect significant pressure on logistics capacity, from transportation to warehousing
  - As other organizations will be scrambling to ramp up activities, a most probable bottleneck will be logistics capacity, which will be at a premium during that time

After we introduce a stress or disruption in the network, the simulation will help us determine if the network can run in a sustainable fashion for a pre-defined period of time, while adjustments can be made. We can also then introduce the proposed adjustments to understand their impact and feasibility.

# 6.  Conclusion

The Covid-19 pandemic has made the risks of not knowing your supply chain network very apparent. Further, it cannot be overstated that the strategically critical defense supply chain needs to have a well-defined framework in place for identifying and mitigating complex risks well ahead of time. Especially as the world is oscillating between a complete shutdown of consumption, production to a sudden increase in demand leading to several bottlenecks arising in the supply chains. There are several suppliers at various tiers of visibility who cater to the needs of both the civil supply chain and the defense supply chain, and the huge variability of demand, leading to some suppliers shutting down and others struggling to match the capacity demand, which can dramatically increase the risk posed by such entities at different levels.

However, this junction also provides an opportunity for accelerated adoption of digitalization by various actors in the supply chain, increasing the depth of data collection and to integrate the data with the methodologies of risk mitigation. These methodologies provide a robust framework for powering a supply chain digital twin using a supply chain network mapping, and further harnessing these mappings using simulation techniques to perform stress tests and finally achieve effective outcomes for the defense supply chain systems at the most granular level.

**References:**

1.      Bugert, Niels; Lasch, Rainer (2018) : Supply chain disruption models: A critical review, Logistics Research, ISSN 1865-0368, Bundesvereinigung Logistik (BVL), Bremen, Vol. 11, Iss. 5, pp. 1-35, http://dx.doi.org/10.23773/2018_5.

2.      Stauffer, D., 2003. Supply Chain Risk: Deal With It. [online] HBS Working Knowledge. Available at: <https://hbswk.hbs.edu/item/supply-chain-risk-deal-with-it>.

3.      Simchi-Levi, D. and Simchi-Levi, E., 2020. We Need a Stress Test for Critical Supply Chains. [online] Harvard Business Review. Available at: <https://hbr.org/2020/04/we-need-a-stress-test-for-critical-supply-chains>.

4.      Y. Choi, T., Rogers, D. and Vakil, B., 2020. Coronavirus Is a Wake-Up Call for Supply Chain Management. [online] Harvard Business Review. Available at: <https://hbr.org/2020/03/coronavirus-is-a-wake-up-call-for-supply-chain-management>.

5.      Fan Y., Heilig L., Voß S., 2015. Supply Chain Risk Management in the Era of Big Data. In: Marcus A. (eds) Design, User Experience, and Usability: Design Discourse. Lecture Notes in Computer Science, vol 9186. Springer, Cham. https://doi.org/10.1007/978-3-319-20886-2_27

6.      Simchi-Levi, D., 2020. Three Scenarios to Guide Your Global Supply Chain Recovery – MIT Sloan Management Review. [online] Sloanreview-mit-edu.cdn.ampproject.org. Available at: <https://sloanreview-mit-edu.cdn.ampproject.org/c/s/sloanreview.mit.edu/article/three-scenarios-to-guide-your-global-supply-chain-recovery/amp>

7.      Jain, Sanjay & Leong, Swee. (2005). Stress testing a supply chain using simulation. Proceedings - Winter Simulation Conference. 2005. 1650-1657. 10.1109/WSC.2005.1574435.

8.      Philip Nuss, T.E. Graedel, Elisa Alonso, Adam Carroll, Mapping supply chain risk by network analysis of product platforms, Sustainable Materials and Technologies, <https://doi.org/10.1016/j.susmat.2016.10.002>

9.      Klapper, L.S., N. Hamblin, L. Hutchison, L. Novak, and J. Vivar. 1999. Supply Chain Management: A Recommended Performance Measurement Scorecard, Logistics Management Institute

10.     U.S. Department of Defense, Office of the Under Secretary of Defense for

For more information about our  solutions, please visit
www.tcgdigital.com