DETECTING CRIMINAL DISRUPTIONS OF SUPPLY CHAINS

Alok Baveja, Department of Supply Chain Management, Rutgers Business School - Newark and New Brunswick, Rutgers University, Piscataway, NJ, 08854, baveja@business.rutgers.edu

Weiwei Chen, Department of Supply Chain Management, Rutgers Business School - Newark and New Brunswick, Rutgers University, Piscataway, NJ, 08854, wchen@business.rutgers.edu

Dennis Egan, CCICADA Center, Rutgers University, Piscataway, NJ 08854, deegan@dimacs.rutgers.edu

Aman Goswami, Department of Supply Chain Management, Rutgers Business School - Newark and New Brunswick, Rutgers University, Newark, NJ, 07102, ag1814@business.rutgers.edu

Peter March, Department of Mathematics, Rutgers University, Piscataway, NJ 08854, pm630@math.rutgers.edu

Benjamin Melamed, Department of Supply Chain Management, Rutgers Business School - Newark and New Brunswick, Rutgers University, Piscataway, NJ, 08854, melamed@business.rutgers.edu

Christie Nelson, CCICADA Center, Rutgers University, Piscataway, NJ 08854, cnelson@dimacs.rutgers.edu

Fred Roberts, CCICADA Center, Rutgers University, Piscataway, NJ 08854, froberts@dimacs.rutgers.edu

ABSTRACT

Criminals tend to take advantage of widespread disturbances like the COVID-19 pandemic to disrupt supply chains. Through case studies from the pharmaceutical and medical device industries, we present a rigorous methodology to identify such disruptions and suggest promising mitigation strategies. Our generalizable approach provides the Department of Homeland Security, other government agencies, and private sector with a framework for (1) constructing supply chain maps with physical and information flows, (2) posing what-if questions regarding "optimal" ways to disrupt supply chain performance, (3) making supply chains more resilient to disruptive attacks, (4) mitigating attacks in-progress, and (5) restoring attacked supply chains.

Keywords - supply chain, criminal disruptions, pharmaceutical industry, medical devices.

INTRODUCTION

The pandemic highlighted our society's reliance on worldwide supply chains for goods and services (Choi et al., 2020; Shih, 2020). The impact of disruptions was dramatic, from Fortune 1000 companies, over 90% of which had their supply chains disrupted (Sherman, 2020), to healthcare workers who were unable to obtain personal protective equipment (PPE), and even to the average consumer who could not obtain essential household items. Criminal organizations seek to take advantage of any crisis, and the pandemic was no exception (FBI, 2020). This paper addresses the development of supply chain models, identifies

effective methods by which criminal organizations may disrupt supply chains, develops indicators and warnings relating to these disruptions, and ultimately recommends actions to mitigate the disruptions. In particular, we have explored two supply chains representing critical homeland security infrastructure, namely, pharmaceutical supply chains and medical device supply chains. The critical importance of these two supply chains was demonstrated during the pandemic when consumers experienced shortages of medicines, ventilators, PPE, and the like (Ranney et al., 2020; Cohen and van der Meulen Rodgers, 2020). Importantly, many of our findings extend naturally to supply chains in general. In this paper, we present our generalizable methodology as well as widely-applicable lessons learned.

Criminal organizations have previously disrupted and manipulated supply chains for financial gain and other reasons, and they will continue to do so (Moosavi et al., 2022). Such disruption and manipulation may take many forms, such as blocking one or more elements of a supply chain to demand ransom, inflicting physical damage on a supply chain target, creating supply delay or uncertainty, motivating a redirection to alternative suppliers, injecting adulterated material into the supply chain and/or removing genuine materials. Consequently, there has been a dramatic increase in attention paid to supply chains, their impact on the global economy, and their vulnerability to disruptions (Duong and Chong, 2020). The effects of supply chain disruptions or manipulations are magnified during times of global crisis, as already fragile systems and populations come under additional stress (Craighead et al., 2020). In Rana et al. (2022) and Patel et al. (2023), other members of our team have developed models of criminal organization capability to disrupt supply chains; together we have studied the worst-case disruptions possible given a fixed disruption budget available to a criminal organization and pre/post disruption mitigation strategies for these worst-case scenarios.

Our modeling methodology includes a supply-chain map consisting of a focal firm of interest and its external linkages. The various disruptions are overlayed by location and type on this supply-chain map such as that of Figure 1. Through extensive consultation with subject-matter experts from industry, we have developed a modeling methodology that incorporates supply chain operations and various disruptive vectors for medical-device and pharmaceutical supply chains. Specifically, we have created a framework that allows us and other members of our team to simulate likely disruption or manipulation scenarios, quantify associated indicators of impact on the supply chain, and quantify the efficacy of mitigation strategies. The subsequent analysis of these specific supply chain models helps to identify plausible attack points, develop warning indicators about a pending, active, or past attack, and provide recommendations to mitigate identified vulnerabilities and reduce attack impacts. The resulting methodology can then be applied to other supply chains as needed.

The approach we describe in this paper can be generalized with applicability to other supply chains. It provides the Department of Homeland Security (DHS), other agencies, and the private sector with a framework for building supply chain models, posing what-if questions regarding “optimal” ways to disrupt them given specific amounts and types of resources and know-how, examining how to make supply chains more robust against attacks, identifying and mitigating attacks in progress, and restoring attacked supply chains to their baseline state.

THE FOCAL-CORE SUPPLY CHAIN METHODOLOGY

Modern supply chains are networks where material and information flow among facilities, often globally. Modern supply chains are increasingly complex. Their complexity stems from their size (number of nodes and links in their flow networks), layout (global reach, often spread across continents), and the functional heterogeneity of their nodes (suppliers, customers, facilities, etc.) At best, this complexity makes it challenging to model and analyze supply chains, and at worst, it makes it impossible when critical information is unreliable or unavailable.

Recognizing these difficulties, we developed an approach to supply chains called the *Focal-core Supply Chain Methodology* (*FSCM*) that effectively addresses the challenge of modeling complex supply chains and analyzing the impacts of disruptions on them. Broadly speaking, FSCM partitions the supply chain network into two components. The first component is a subset of nodes and links of primary interest to decision-makers, referred to as the *focal core*. The focal core typically consists of a focal supply chain firm of interest plus its primary supplier and customer tiers. The second component encompasses supply chain nodes outside the focal core, to be referred to as the *focal core's environment*, or the *environment*, for short. The environment comprises secondary/tertiary/… suppliers and customers excluded from the focal core. Figure 1 shows an example FSCM supply chain model for a generic pharmaceutical company which was developed in collaboration with pharmaceutical industry experts and vetted by pharmaceutical supply chain and security experts. It was used in a wide variety of simulation experiments described in Rana et al. (2022) and Patel et al. (2023).

In Figure 1, we consider a generic pharmaceutical focal firm, dubbed Pharma Company that manufactures both solid oral dose (SOD) and injectable (INJ) pharmaceuticals. The facilities of the focal firm are displayed using gray icons. Those of external suppliers and customers use pink icons (trusted suppliers) and red icons (untrusted suppliers). Arrows in Figure 1 represent flows between nodes, for example, information flows in black and material flows in blue (trusted) or red (untrusted). Grey diamonds represent testing nodes, where material or items tested can be classified as "goodput" (passed testing) or "badput," (failed testing) or "rework", and triangles represent inventories, where triangles feeding into nodes represent Make-to-Stock inventories (managed by ordering a supply that raises the current inventory level to a target level whenever it hits or down-crosses a reorder point level), and others are passive (unmanaged) inventories. Hand grenades correspond to various types of disruptions, and they are labeled with a code that corresponds to a classification of disruptions that was built up from real examples and company experts.

In Figure 1, end-customers order SOD and INJ daily from a pool of hospitals and pharmacies, which are replenished by the focal-firm's distribution center and a wholesaler. The focal firm's distribution center places monthly orders of SOD and INJ with the pharma company. On order receipt, the pharma company sends appropriate orders to its external suppliers that provide raw material, excipients (substances that contribute to long-term stability of a drug or vaccine, and that may aid in its administration, e.g., binders, aerosols, coloring, flavoring, or lubricants), and packaging. Manufacturing consists of 3 key steps. First, active pharmaceutical ingredients (API) are produced from raw material, then drugs are produced by mixing API with excipients and finally, the drugs are packaged. After each step, testing identifies and removes badput, and allows goodput or rework to proceed on. Some of the manufacture is contracted out to contract manufacturing organizations (CMOs).

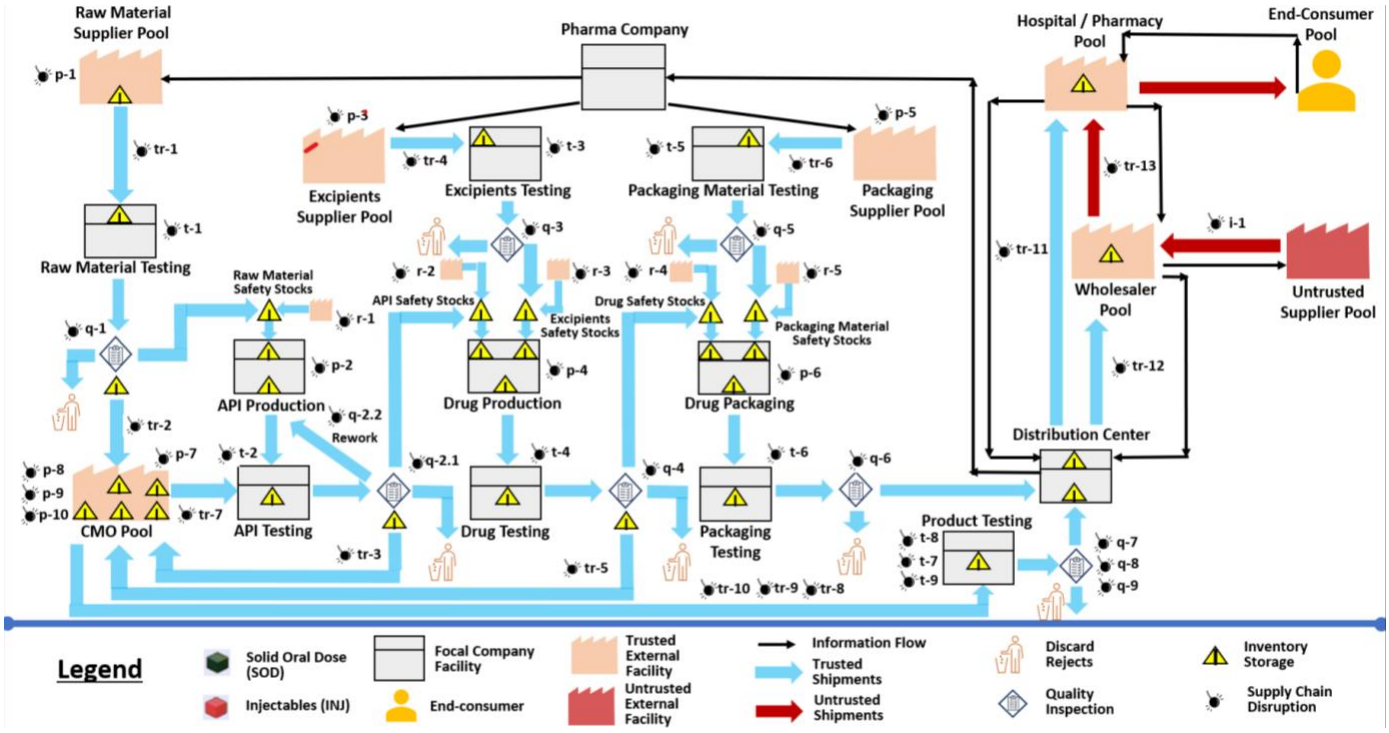

Figure 1: FSCM Map of Operations & Disruptions: Pharma Company

In Figure 2, we show a medical-device supply chain with a focal firm, dubbed MedTech Company. The meaning of the icons is the same as before, except that yellow triangles represent Make-to-Stock inventories and beige triangles represent passive inventories. However, here there are two categories of medical devices being manufactured: electronic equipment (EE) units, such as medical monitors, and delivery system (DS) units, such as catheters. A treated patient needs full kit (1 EE unit and 1 DS unit). EE units can be reused over their lifetime, and they may break down and be repaired, but DS units are discarded after one use. If an EE unit breaks down, the patient gets a replacement, if available, or waits for one.

In Figure 2, patients arrive at the hospital pool and are assigned a full kit, if available, or wait for a full kit to become available. After treatment, patients leave the system and return their EE unit. EE and DS productions are separate operations. EE production is completely outsourced to a CMO pool while DS production is split between the focal firm and a CMO pool. Both production operations use raw material and packaging from external suppliers, and the production and testing steps are self-explanatory. Finished EE and DS products are sent to 4 distinct warehouses as indicated by the material flow arrows. The hospital is replenished by these warehouses via Make-to-Stock inventories of EE and DS units.

The FSCM approach models the focal core in considerable detail and aggregates the environment components for simplicity. Specifically, the environment is modeled as an extra single tier of nodes directly linked to the focal core. This supplemental tier is created by an extensive aggregation of the real-life supply chain in two ways:

1. Aggregation that combines like-nodes into a single pool node. For example, multiple distinct suppliers of the same material are modeled by a single supplier pool.
2. Aggregation by combining the entire upstream supply chain that lies wholly in the environment into a single node. For example, distinct suppliers in tiers upstream of a single supplier pool are merged into a pool. Downstream distribution tiers to end-customers are handled similarly.

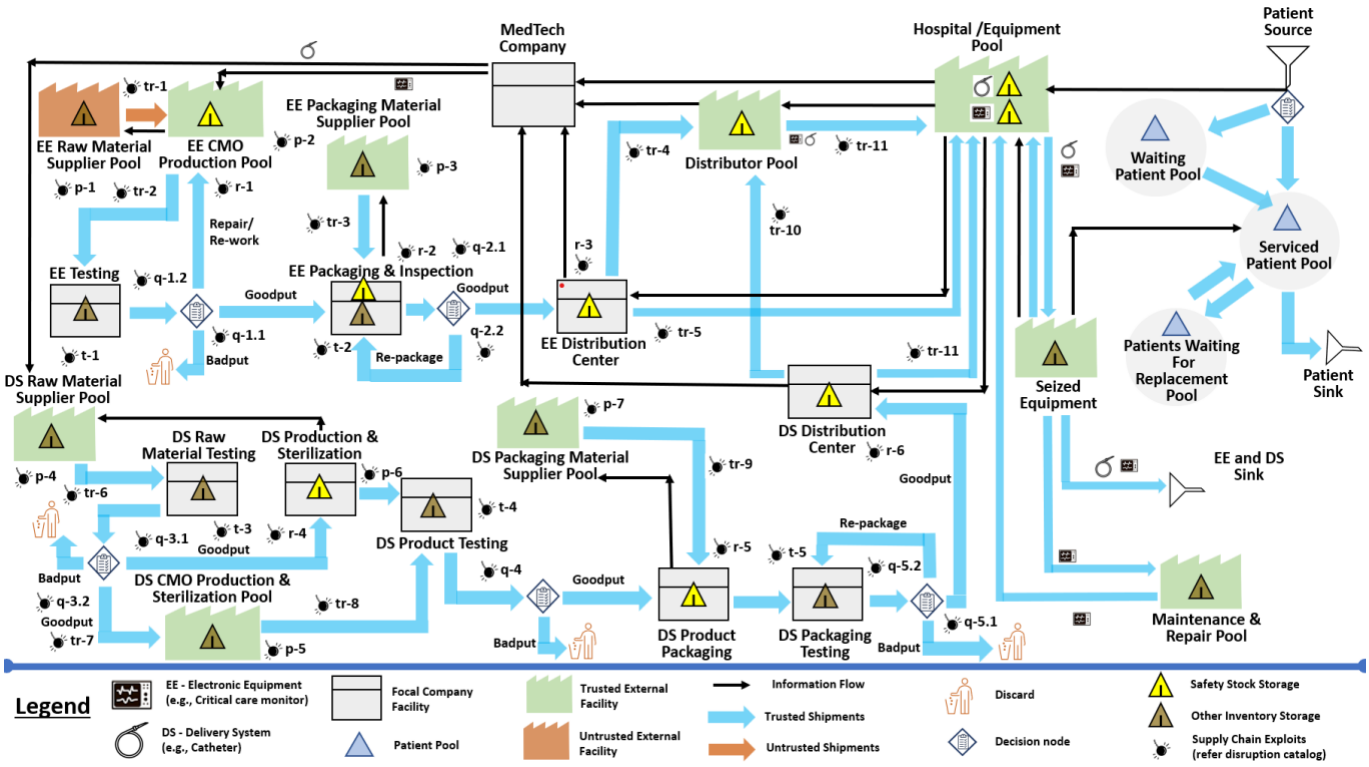

Figure 2: FSCM Map of Operations & Disruptions: MedTech Company

3. Aggregation that combines like-nodes into a single pool node. For example, multiple distinct suppliers of the same material are modeled by a single supplier pool.
4. Aggregation by combining the entire upstream supply chain that lies wholly in the environment into a single node. For example, distinct suppliers in tiers upstream of a single supplier pool are merged into a pool. Downstream distribution tiers to end-customers are handled similarly.

The selection of the focal-core component is a modeling decision driven by two considerations. The first is the availability of sufficient reliable information to parameterize the model, and the second is the computational size of the resultant model.

Typically, information about the supply chain under study is obtained from current or past employees of a supply chain company. Such information includes key parameters that include travel times, testing delays, sizes of inventories, etc., and such parameters then inform various simulations of supply chain performance

under “normal” (baseline) or disrupted conditions. Often employees who aid in supply chain construction and parametrization are familiar only with a part of the broader supply chain in which their focal firm is embedded, and, therefore, information about the supply chain beyond that subset is not readily available. Thus, that subset, minus the farthest upstream and downstream tiers of the focal firm, is a natural choice of the focal core component of the model, with the tiers farthest from it becoming the focal core’s environment.

The second consideration regarding the computational size of the resultant model is standard practice in simulation modeling. To gain modeling clarity and actionable insights, the model is run multiple times to compute various performance metrics. These simulation runs require computational resources that can grow significantly with the size and complexity of the model. Thus, the model size must be limited to obtain effective and timely results, which factors into choosing the model’s focal core and environment. The following is an outline of the FSCM’s steps for modeling a supply chain:

1. Assemble an advisory group of subject-matter experts that can provide information on the supply chain’s network structure and data for model parameters. All subsequent steps are carried out in close collaboration with this group.
2. Identify the focal core and environment of the supply chain model, including the types of entities flowing through it, such as raw materials, subproducts, information, and quality control inspection.
3. Create a supply chain map – a diagram showing the supply chain layout, encompassing all nodes and their directional links. Nodes typically represent fixed assets like production, testing, and warehousing facilities, while links represent transportation routes and information flows. For each node and link, determine how quantities will be measured, for example, in pounds, hours, or as a probability.
4. Based on literature research and consultation with security experts from the aforementioned advisory group, compile a preliminary list of disruptions to be modeled, organized by location (the node or link of possible occurrence) and impact type (for example, decreasing production rate, increasing transportation time, or absence of critical materials). Identify the model parameter impacted by each disruption – for example, changes in mean unit production time, mean transportation time or probability of quality control rejects.
5. Overlay all possible disruptions on the supply chain map, placing an icon and a disruption code at each location where the disruption can occur. The supply chain map facilitates editing the preliminary list of disruptions from the previous step.
6. Using interview sessions with members of the advisory group of experts, parameterize the model with numerical data that correspond to the supply chain in approximate equilibrium or baseline operation of the supply chain. Typical data include delay distributions at supply chain nodes, unit production delay, shipment travel time along links, probability of rejected units after a testing step, replenishment lead times of stocks, and probabilities of routing units to particular links. In practice, a running simulation model is considered to have entered an approximate equilibrium regime – or baseline operation - when key statistics, like production rates and shipment times, stabilize over time. Before any experiments are performed, the model should be run for a so-called “warm-up period” to bring it into stable baseline operation. Since supply chains are evolving rapidly, and since the numerical data is only estimated, the data should be updated regularly and analyses with the data should take into account its approximate nature.

7. Define model-generated statistics that serve as performance metrics of interest to decision-makers or for gaining insights into supply chain operations. Examples of such statistics include time series and histograms of inventory levels, lead times of shipments, and inventory stock-out periods, as well as their summary statistics (means, variances, coefficients of variation, etc.).
8. Create the supply chain simulation model. Run it in baseline mode and then, separately, run it in disrupted mode by injecting one or more disruptions into the baseline model. Measure performance metrics of interest, such as those identified in step 7, including disruption-related metrics such as the fraction of time during which the inventory stocked out or the time to recover from disruptions. For example, if a disruption lowers or depletes an inventory level below a baseline level, measure the time it takes the inventory to return to the baseline level.
9. Perform scenario experiments using simulation runs to evaluate the severity of disruptions based on their computed disruption-related metrics. Identify the most vulnerable points in the supply chain and devise robust mitigation strategies based on such vulnerabilities and/or from interviews with the advisory group of experts or from the literature. Key mitigations can either be pre-disruption or post-disruption and include increasing the levels of safety stocks at production nodes to sustain downstream flows longer by increasing the reorder points target levels of Make-to-Stock inventories, and by securing stand-by manufacturing capacity via outsourcing to contract manufacturing organizations (CMO pools).
10. Perform scenario experiments on the model using simulation runs, with mitigations included, and assess their effectiveness in returning the supply chain to baseline operation.

INSIGHTS

The value of FSCM has been demonstrated by applying it to two industrial supply chains: those of a pharmaceutical company and a medical device company. The simulation models were constructed and parameterized with the aid of respective industry expert groups, and experiments were conducted with various disruption scenarios, starting from varying baseline states. These experiments analyzed the efficacy of detecting and mitigating injected disruptions using multiple supply chain metrics.

The entire exercise of mapping the supply chain, creating the simulation model, and collaborating with colleagues in running simulation experiments and conducting a subsequent analysis helped us gain valuable, actionable insights, many of which are generalizable to other supply chains. We found a recurring pattern of insights across the two supply chains studied, helping to validate the robustness of our findings, consistent with the methodology of building theories from case-study research (Eisenhardt, 1989). We share these insights in three broad categories: Operational Insights, Managerial and Planning Insights, and Strategic Insights.

Operational Insights

1. Making a supply chain more visible and transparent is vitally important in identifying potential vulnerabilities (Christopher and Lee, 2004). One key process insight was that despite the various idiosyncrasies of pharmaceutical and medical device supply chains, there was enough commonality of structure that robust conclusions could be drawn from a generic supply chain. This suggests that supply chains for specific applications can be built by customizing, adapting, or updating a generic model. A visual representation of linkages among the focal company, contract manufacturing organizations

(CMOs), suppliers, distributors, and customers were invaluable to understanding flow patterns, bottlenecks, safety measures, and vulnerabilities. Visibility and transparency of the external components in the environment component are as critical as those of the internal components of the focal core. However, this visibility and transparency is not always achieved in practice even for the focal company, let alone a modeler. For the focal company, it can be achieved by forming strategic partnerships with external suppliers and CMOs that leverage collaborative and data-sharing platforms.

2. Numerous parameters are required for an effective supply chain model. However, the precise parametrization, while valuable, is not as important as showing that the real-life parametrization of the model is feasible through proof-of-concept case studies. In addition to quantifying the parameters, it was important to distinguish between parameters of interest versus those that were not under the control of the decision-maker.

3. The propagation patterns of disruptions and their indirect impact on supply chain components were important findings of this study, with disruptions often having cascading impacts downstream from their point of origin. Such cascading disruptive effects underscored the need for sensors/measurements throughout the supply chain, especially in its upstream nodes. It also underscored the importance of using those sensors to develop anomaly detection tools.

4. Anomaly detection is an important component of a disruption warning system. Such anomaly detection relies on the multiplicity of sensors throughout the supply chain. An Anomaly Detection System (ADS) needs to be carefully calibrated and adjusted empirically, keeping in mind "known" and "knowable" threats. The efficacy of an early warnings and alert system depends on the empirical and real-time adjustment of ADS parameters. Such a real-time ADS system is very important, for example, in medical supply chains, where hospitals may depend on these devices to provide critical care to patients. Linking the ADS system to a catalog of threats provides a mechanism for the early detection of a variety of anomalies throughout the supply chain.

5. The quantity of safety stocks is determined based on factors such as replenishment lead times, costs, and the number of suppliers (Amirjabbari and Bhuiyan, 2014). It is important that secondary, tertiary, and earlier disruptive risks for all materials be taken into account when determining safety stock parameters such as reorder levels and target levels, and so modification of these parameters can play a role in responding to varying levels of disruptive threats.

6. Because they ensure coordination and synchronization in the supply chain, information flows are an essential and integral component of supply chain strategy. Just as important as maintaining adequate safety stocks and understanding how and when to draw them down or replenish them is to include continuous risk assessment by both internal and independent external parties, such as suppliers and CMOs, through robust and real-time information-sharing practices. The modeling and simulation we have carried out provide a deeper understanding of information flows' critical role within pharmaceutical and medical device supply chains. Information flows in the focal company supply chain model support physical/material flows, so they need to be reliable and accurate. The continual availability of accurate information is especially critical to the effective functioning of most modern supply chains. Accuracy of and trust in data are critical in monitoring a supply chain. They are also critical in getting reliable indications of a disruption in progress or early warnings of planned ones. A disruption that replaces accurate data with false data could be difficult to discover and could easily lead to further major disruptions. A disruption that creates distrust in underlying data could accomplish much the same thing. Therefore, the importance of reliable information flows in supply chains, especially those such as in pharma and medical devices where compliance is paramount, cannot be overstated.

7. Protection against cyberattacks in the pharmaceutical and medical device industries has come to have much more prominence in recent years. For example, a report (Health-ISAC, 2022) aimed at pharmaceutical CISOs emphasizes the various vulnerabilities to such attacks. Cyberattacks could impact components from testing facilities to inventories and affect both factory operation and identification/response to disruptions (Williams and Woodward, 2015). Discrepancies between actual and digital data can give early warning of a problem. Systems to identify such discrepancies could help expedite identification of data disruptions, missing inventory, including safety stocks, etc. While there is emphasis on cyber defense for core focal company processes, defense could be extended to agreements with suppliers and CMOs, such as requirements for more testing, vetting of employees, and regular reporting on cyber disruptions. Such cooperation across the entire supply chain enterprise is imperative; a single weak link in the network can render the entire supply chain vulnerable to cyber threats.

Managerial and Planning Insights

1. The efficacy of early warning systems and indicators depends on the availability of real-time data from the entire supply chain network. Over-reliance on data at finished goods nodes and lack of sufficiently many "sensors" at upstream nodes of the supply chain could result in detection delays of disruptions that could result in significant and pervasive performance deterioration and adversely impact the recovery time metric. A key managerial insight is the installation of multiple "sensors" throughout the supply chain and continuous monitoring of key indicators such as inventory levels, waiting times, testing-node outputs, flow times, etc. (Lechler et al., 2019). Note that sensors do not have to be physical devices. Enhanced visibility of supply chains could be garnered from sensor equivalents, such as increased vetting of suppliers and more extensive testing at all production phases.
2. High levels of safety stock inventories are important in both the pharmaceutical and medical device (Talluri et al., 2004). While serving an important role in avoiding production disruptions and maintaining the continuity of supply, these inventories can mask disruptions and prevent their early detection, potentially increasing the scope of the disruption's impact (Sheffi and Rice Jr, 2005). Therefore, a key actionable managerial insight is the importance of directly keeping track of safety stocks by enhanced sensor systems or by reliable periodic reviews. Such direct monitoring of safety stocks can enable early detection of a disruption when the depletion of safety stocks occurs at an anomalous rate. More generally, there is significant value to continuous monitoring of key indicators such as inventory levels, waiting times, testing-node outputs, flow times, etc. Because disruption effects propagate to other nodes, having a variety of "sensors" at strategic locations is important. The first anomaly detected may not be the most important one, but it is important as an early indicator and warning. The effect of not having sensors at upstream nodes in the supply chain can lead to longer times to detect anomalies at downstream nodes. Operationally, installing and monitoring these sensors will require an upfront and ongoing commitment of resources. However, leveraging existing technology could keep the costs low, especially with an increasing scale of deployment, offering a high benefit-to-cost ratio.
3. There is an inherent tradeoff between sensitivity and specificity when designing early warning and alert systems. Pharmaceutical supply chains are often built to maintain production continuity to maximize sales revenues. This may make the organization less willing to accept the cost of false alarms, leading to "missed" early warnings of disruptions. Accepting more false alarms has a cost, but it is important

to recognize that sometimes this cost is much less than that of a real disruption. Such recognition requires an organizational and managerial shift in mindset.

4. Anomalous order levels should trigger review and possible intervention. Too often, anomalous order levels are noted by sales teams in a company but not shared with the security teams in a timely manner. Pharmaceutical and medical device companies and their supply chain partners would benefit from putting together dedicated inter-organizational teams that collaborate on studying these anomalies. Such teams could also continuously update information about criminal organizations' past, current, and emerging capabilities, including embedding subpar devices in developing countries where regulatory standards are not in place.
5. The supply chain models we built consist of a number of CMOs. CMOs can provide backup capacity in the form of supply option contracts, to be exercised for a speedy response in disruption emergencies, though at an additional cost. Analysis suggests that even when these backup CMOs have limited capacity compared to the focal company's capacity, they could still play an important role in reducing the severity and duration of disruption impacts. However, backup CMOs would not be as effective should there be a long delay in detecting a disruption and exercising the option contract. Indeed, planning for backup CMOs should be combined with early detection and communication systems to provide a robust mechanism to mitigate disruptions.

Strategic Insights

1. In highly regulated industries, such as the pharmaceutical and medical device industries, significant effort and resources are expended to prevent, track, and remediate external failures. Not only do failures of any kind accrue a high financial burden, but they also adversely impact the company's long-term brand and its compliance status with government agencies (Medical Plastic News, 2022; UBS, 2021). Accordingly, our models for both industries incorporated extensive testing nodes throughout the supply chain network consistent with common industry practice. As with safety stocks, compromising the availability or effectiveness of testing competencies could be a source of significant disruption. Disruption to the reliability of testing could seriously impact supply chain operations. Ongoing risk assessment and periodic checking of the efficacy of testing at various supply chain components are critical safeguards for companies to put in place. Such safeguards should not be limited to the focal company alone but should also involve a comprehensive risk assessment of procedures and data at external parties, such as raw material suppliers and CMOs, which could be sources of significant vulnerabilities.
2. Both industries we studied maintain high inventory levels due to a variety of factors, such as the need to maintain the availability of products essential to health, regulatory pressures, perishable inventories, long manufacturing lead times, limited supply options, and maximization of sales during patent life cycles. However, these safety stock inventories vary considerably across components. The parameters of safety stock inventories were carefully calibrated across our model nodes as per industry practices, and they provide important management tools for development of pre- and post-disruption mitigations.
3. In both pharmaceutical and medical device industries, testing and maintenance practices of safety stock inventories are important strategic areas of strength on which the industry relies for effective functioning. Because of their strategic importance, compromising the availability or effectiveness of these competencies, severally or collectively, can be a source of significant disruption. Disrupted

reliability of testing and/or unavailability of safety stocks could seriously impact supply chain operations.

4. When designing and running simulation experiments or exercises, we found that proper measurement of the impact of disruptions calls for appropriate choices of metrics and criteria for measuring performance quality under a disruptive scenario. Such metrics and criteria can help to compare the impacts of various disruptions at various supply chain nodes under attack by criminal organizations. The standardization of such metrics and criteria and corresponding policy guidance from government agencies could be very useful to supply chain managers.

CLOSING COMMENTS

This paper reflects the development and use of a generic supply chain modeling technology that addresses key homeland security goals of protecting critical infrastructure, detecting threats, mitigating, responding to, and recovering from disruptions, protecting the availability and integrity of information, and enabling effective physical and cyber resilience. The methodological innovation in this work centers on taking a focal-company viewpoint while incorporating upstream and downstream external linkages through judicious aggregation. This modeling methodology was specifically designed for broad applicability across a variety of supply chains. Besides the pharmaceutical and medical device supply chain case studies presented in this paper, we have also tested the applicability of this methodology to satellite solar arrays and food production supply chains. Importantly, the technology developed in this research can incorporate disruptive vectors directly into the supply chain model. In turn the resultant model can serve as the basis of a multifaceted simulation model where physical and information flows can be studied under various disruptive scenarios, allowing decision-makers and planners from the private sector and government agencies to run and learn from what-if experiments, gaining insights such as those we have described. With a growing number of physical and cyber threats on a multitude of critical supply chains, we think technological innovations such as the one developed in this paper can help build resilient infrastructure systems that can prevent, detect, and rapidly recover from disruptive attacks.

ACKNOWLEDGEMENTS

This project has been funded in whole or in part with Federal funds from the Department of Homeland Security under BOA No. 70RSAT18G00000001, task order no. 70RSAT21FR0000127. The content of this publication does not necessarily reflect the views or policies of the Department of Homeland Security, nor does mention of trade names, commercial products, or organizations imply endorsement by the U.S. Government. The authors also wish to thank their collaborators Andrew Crooks, Carlotta Domeniconi, Jim Jones, Hamdi Karzak, Sean Luke, Vladimir Menkov, Raj Patel, and Abhisekh Rana for their key contributions to the simulations, criminal organization models, and experiments that are not described here but helped to contribute to the insights and conclusions summarized.

REFERENCES

Amirjabbari, B. and Bhuiyan, N., 2014. Determining supply chain safety stock level and location. *Journal of Industrial Engineering and Management (JIEM)*, *7*(1), pp.42-71.

Choi, T.Y., Rogers, D. and Vakil, B., 2020. Coronavirus is a wake-up call for supply chain management. *Harvard Business Review*, *27*(1), pp.364-398.

Christopher, M. and Lee, H., 2004. Mitigating supply chain risk through improved confidence. *International journal of physical distribution & logistics management*, *34*(5), pp.388-396.

Cohen, J. and van der Meulen Rodgers, Y., 2020. Contributing factors to personal protective equipment shortages during the COVID-19 pandemic. *Preventive medicine*, *141*, p.106263.

Craighead, C.W., Ketchen Jr, D.J. and Darby, J.L., 2020. Pandemics and supply chain management research: toward a theoretical toolbox. *Decision Sciences*, *51*(4), pp.838-866.

Duong, L.N.K. and Chong, J., 2020. Supply chain collaboration in the presence of disruptions: a literature review. *International Journal of Production Research*, *58*(11), pp.3488-3507.

Eisenhardt, K.M., 1989. Building theories from case study research. *Academy of management review*, *14*(4), pp.532-550.

FBI, "FBI and Secret Service Working Against COVID-19 Threats," 2020, https://www.fbi.gov/news/press-releases/fbi-and-secret-service-working-against-covid-19-threats

Health-ISAC. "Securing the Modern Pharmaceutical Supply Chain: A Guide for CISOs in an Age of Disruption, 2022, https://h-isac.org/securing-the-modern-pharmaceutical-supply-chain/

Lechler, S., Canzaniello, A., Roßmann, B., von der Gracht, H.A. and Hartmann, E., 2019. Real-time data processing in supply chain management: revealing the uncertainty dilemma. *International Journal of Physical Distribution & Logistics Management*, *49*(10), pp.1003-1019.

Medical Plastic News. "Overcoming supply chain disruptions in medical device manufacturing," 2022. https://www.medicalplasticsnews.com/medical-plastics-industry-insights/medical-plastics-insights/overcoming-supply-chain-disruptions-in-medical-device-manufa/

Moosavi, J., Fathollahi-Fard, A.M. and Dulebenets, M.A., 2022. Supply chain disruption during the COVID-19 pandemic: Recognizing potential disruption management strategies. *International Journal of Disaster Risk Reduction*, *75*, p.102983.

Patel, R., Rana, A., Luke, S., Domeniconi, C., Kavak, H., Jones, J. and Crooks, A., 2023, May. Simulation and Optimization Techniques for the Mitigation of Disruptions to Supply Chains. In *2023 Annual Modeling and Simulation Conference (ANNSIM)* (pp. 134-145). IEEE.

Rana, A., Kavak, H., Crooks, A., Luke, S., Domeniconi, C. and Jones, J., 2022, September. Mitigation of Optimized Pharmaceutical Supply Chain Disruptions by Criminal Agents. In *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation* (pp. 13-23). Cham: Springer International Publishing.

Ranney, M.L., Griffeth, V. and Jha, A.K., 2020. Critical supply shortages—the need for ventilators and personal protective equipment during the Covid-19 pandemic. *New England Journal of Medicine*, *382*(18), p.e41.

Sheffi, Y. and Rice Jr, J.B., 2005. A supply chain view of the resilient enterprise. *MIT Sloan management review*.

Sherman, E. "94% of the Fortune 1000 are seeing coronavirus supply chain disruptions: Report," 2020, https://fortune.com/2020/02/21/fortune-1000-coronavirus-china-supply-chain-impact/

Shih, W.C., 2020. Global supply chains in a post-pandemic world. *Harvard Business Review*, *98*(5), pp.82-89.

Talluri, S., Cetin, K. and Gardner, A.J., 2004. Integrating demand and supply variability into safety stock evaluations. *International Journal of Physical Distribution & Logistics Management*, *34*(1), pp.62-69.

UBS. "Medical device sales recovering from COVID-19 disruption," 2021. https://www.ubs.com/global/en/wealth-management/our-approach/marketnews/article.1536314.html.

Williams, P.A. and Woodward, A.J., 2015. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, pp.305-316.