Supply Chain Threats and Countermeasures: From Elicitation through Optimization

Weihong "Grace" Guo
Rutgers University
wg152@soe.rutgers.edu

Paul Kantor
Paul B Kantor, Consultant
paulbkantor@gmail.com

Elsayed A. Elsayed
Rutgers University
elsayed@soe.rutgers.edu

Eric Rosenberg
Georgian Court University
erosenberg@georgian.edu

Rong Lei
Rutgers University
rl839@scarletmail.rutgers.edu

Sachin Patel
Rutgers University
sap357@scarletmail.rutgers.edu

Brendan Ruskey
Rutgers University
bjr110@scarletmail.rutgers.edu

Fred S. Roberts
Rutgers University
froberts@dimacs.rutgers.edu

Abstract

There are many checklists for improving supply chain resilience under different threats, but a lack of concrete procedures to rigorously assess and select among countermeasures (CMs). We present a novel process and method to elicit the needed information to identify CMs and assess their ability to reduce risk. We report on the fine-grained analysis underlying an effective simulation developed to model both the impact of threats and the impact of alternative CMs in the information and communication technology supply chain subject to disruptions due to natural hazards. We also describe the coarse-grained descriptions needed to elicit risk reduction estimates from subject matter experts, and the problems of integrating these two approaches, bottom up, and top down, to support management decisions to choose an optimal set of CMs given a limited budget.

1. Introduction

1.1. Problem and Approach

Every nation is increasingly aware that information and communication technologies are sourced from around the world, with the best performance cost ratios often coming from sources that are vulnerable to a number of threats. The information and communications technology (ICT) products and services supply chain is vulnerable at every point from the design of chips to the moment that equipment or software is installed. The U.S. is responding, particularly through the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and specifically CISA's Information and Communications Technology Supply Chain Risk Management Task Force Working Group 2: Threat Evaluation. This group has identified nine categories of threats to the ICT supply chain and has developed specific threat scenarios for each threat category that are detailed enough to be useful to industry and government decision makers. The Working Group 2 report [1] has served as a starting point for this project.

We report on a methodology to quantify the impact, measured by reduction in risk associated with specific countermeasures (CMs) to threat scenarios. With the help of CISA and industry experts from a project Advisory Board, we have selected and specified three threat scenarios that span many kinds of issues that are representative of the major issues raised in the Working Group 2 report and from which our work should be readily generalizable to the other threats of interest. The first involves natural hazards: floods, storms, earthquakes. They are modeled at the level of plants and interconnections. The second scenario involves counterfeit materials. They are modeled by a flow of individual parts or components. The third scenario involves problems of "onboarding" a new supplier. This represents problems of financial stability, technical competence, intellectual property rights, and geopolitical factors. Our methodology has three components: elicitation of CMs and risk reduction estimates from subject matter experts (SMEs), network modeling and simulation of the supply chain, and use of optimization tools to choose an optimal set of CMs. We report on application of our methods to the natural hazards threat. While our methodology can be easily extended to the other two threats we have studied, the technical details, such as changing from a plant-based

simulation to an agent-based model for parts requires detailed expansion of the description that is beyond the scope of a short paper.

We gather input from SMEs in a Zoom-based focus group approach that includes development of consensus risk reduction estimates. From these consensus estimates, sophisticated computer simulation using the anyLogistix tool [2] generates hundreds of random examples. This "Monte Carlo" method is the gold standard for uncertainty in finance and climate. To identify best decisions, simulations are tied to an optimization algorithm using Mixed Integer Programming that considers many possible combinations of protections. For any given budget it finds the best allocation of limited funds.

This project is developing a methodology that we hope will be of use to CISA, other components of DHS, and the private sector. Our tools provide new approaches to eliciting expert assessments of relative risk reduction of different CMS. Our network models and simulations for supply chains and our optimization models for selecting the most effective set of CMs should be of interest to those concerned with understanding the risk reduction of different mitigation strategies for supply chain disruptions. The results should provide some insight about supply chain threats such as those in the three chosen scenarios, but also more generally to a wide variety of scenarios and to a wide variety of types of supply chains, not just for ICT.

The elicitation process, network modeling and simulations of supply chains, and optimization tools both inform and are informed by each other. Section 2 describes the elicitation procedure. The details of the network models are presented in Section 3, while the approach we have developed for optimization appears in Section 4. We discuss the challenges of integrating these three project components into a single coherent tool for planning and decision making, and some possible extensions of this work, in Section 5.

1.2. Related Literature

This project has benefited from an extensive literature on supply chains and supply chain resiliency; elicitation of risk and risk reduction; modeling and simulation; and approaches to risk and risk reduction in the three scenarios of interest. We mention selected work that has influenced our own approach.

Supply Chains/Scenarios/Threats: Recent relevant supply chain risk/disruption reviews are presented in [3] and [4]. An earlier work that used extensive qualitative methods is in [5]. However, the literature lacks information on the quantitative **impact** of specific mitigations and CMs.

The key source for our selection of threats/scenarios is the analysis of CISA Working Group 2 [1]. There is also an enormous literature on CMs. This literature proposes checklists, often with anecdotal evidence about some mitigation, leaving users to select their own portfolios for implementation. We have found that the literature on threats to supply chains under the three scenarios of interest was the most helpful part of the supply chain literature, so we describe it here.

Natural Disasters: Public sources such as [6] and reports from FEMA (Federal Emergency Management Agency), ASCE (American Society of Civil Engineers), and NOAA (National Oceanographic and Atmospheric Administration) provide useful information regarding multiple hazards. Data analytic approaches such as those of [7, 8, 9, 10] have been very helpful in providing ways to quantify and characterize supply chain resilience under multiple natural hazards, helping us develop performance metrics for our simulations.

Counterfeit Parts: The presence of counterfeit products has led to the development of the Suspect Counterfeit database in GIDEP (Government-Industry Data Exchange Program) [11], a very helpful resource. The Electronic Resellers Association (ERAI) is a major resource with the world's largest database of suspect counterfeit and noncomforming electronic parts [12]. The literature also describes best practices for government and industry, e.g., the Navy's Counterfeit Materiel Process Guidebook [13] provides tools for implementing a risk-based counterfeit materiel prevention program such as ours. [14] provides counterfeit risk mitigation strategies and [15] describes challenges of increasing reliance on commercial-off-the-shelf (COTS) components. We build on similar strategies, e.g., different inspection procedures for components from selected vendors or from COTS sources. [16] suggests using different kinds of tests; likewise, our simulations allow for different levels of testing based on questionable behavior. [17] suggests stronger preventive measures, which are reflected in our simulations studying pre-event or preventive CMs as well as post-event CMs. [18] describes what makes a good counterfeit prevention plan and [19] lays out a prototype agent-based simulation that implements an anti-counterfeiting framework. As in our project, the goal is to use such simulations to identify effective anti-counterfeiting policies. However, no prior work similar to our approaches has been reported in the literature.

Onboarding of New Suppliers: The literature lacks quantitative metrics or simulation modeling of the onboarding of new suppliers. The CISA Working

Group 2 description of an onboarding threat scenario emphasizes financial health and early warning signs that a vendor might be dependent on a foreign government for financial support, signs also mentioned in the description of MITRE's Supply Chain Security System of Trust [20]. The literature on counterfeit parts is relevant to the onboarding threat as well. For example, [17] recommends that a vendor's reporting of counterfeit parts be monitored and failures potentially leading to debarring, ideas our models and simulations use. Digital watermarking of physical and digital documents (and components) is among the CMs relevant to the onboarding scenario, with publications such as [21, 22, 23, 24] influencing our work.

Elicitation: There are many reviews of the literature on elicitation, e.g., [25]. When scientific advice is used in government decision making, the traditional approach has been committee discussion, which can result in bias. This was one motivation for development of more structured decision-making processes such as Delphi [26, 27]. Formal procedures for eliciting judgments about risk and risk reduction from experts, and pooling their judgments, can help to quantify risk as well as uncertainty [28]. We started with established procedures for eliciting estimates of risk (e.g., [27]). After reviewing many methods, such as those reviewed in [25] and the ones instantiated in [29] and [30], we adopted a recent method aimed at experts unfamiliar with probabilities [31]. This method extends the classic methods for the combination of probabilities initiated in [32]. The central idea is that distributions need not be well modeled by a well-behaved "Bayesian conjugate distribution," since all down-stream calculations are numerical Monte Carlo simulations. [30] presented a similar idea, although their conceptual framework seeks a parametric form for the distribution. Our elicitation uses extensions of classical methods by [33, 34, 35, 36]. [35] and [36] point out the importance of training experts in making probability judgments, influencing us to include a training component in our elicitation. In our focus groups estimates are aggregated by averaging, as suggested by [32], and also using a generalization of the median concept given by [37].

Our approaches to elicitation of risk and risk reduction are grounded in the large literature on risk management. [38] and [39] present the process of risk management in steps: risk identification, risk assessment, risk mitigation, and situation monitoring. Our work concentrates on the risk assessment and risk mitigation steps – with an emphasis on identifying CMs to reduce risk. [40] points out how to extend this stepwise model to the notion of opportunity, the idea that events can also provide positive impacts, which we do not consider. [41] describes risk as the combination of the severity of the effects and probability of occurrence. This reflects the fact that performance of a supply chain is dependent on changing conditions, some of which (such as occurrence and severity of a natural disaster) are beyond our ability to measure – and something our elicitation processes and our simulation models reflect. Risk reduction occurs in the context of uncertainty. [40] has proposed an interesting framework that reflects the reality that no supply chain will have a static stable equilibrium in a world with a constantly changing environment. Our work also builds on the dynamic nature of supply chains and the idea that risk and risk reduction are dynamic concepts.

Simulation: Simulation allows us to study complex, real-world systems with stochastic elements and to "see" how different scenarios of disruptions and implementations of CMs impact the entire supply chain. Simulation has been widely used for tackling the uncertainties in supply chain networks. [42] reviewed several simulation techniques that quantitatively addresses uncertainty in supply chains. [43] developed a framework of a digital supply chain twin for managing the risks in pre, during, and post disruption stages. [44] proposed a dynamic model for evaluating the service level of supply chains in scenarios with disruptions. Mathematical formulation of the network is difficult since the causes of disruptions and their severities are often random with unknown probability distributions, so a simulation model of the network is a viable and realistic approach to evaluate the dynamic performance of supply chain(s) in virtual environments [45, 46, 47].

Our simulation models include estimates of both the degradation rate and recovery rate in modeling the ability of each node and arc to meet performance levels. These are combined to quantify overall supply chain performance. We compute importance measures for each node or arc, extending the importance measures discussed in [48] to incorporate multiple threat types.

2. Elicitation

Subject Matter Experts (so far 34 interviewed, 18 also in Focus Groups) are recruited in a "snowball" process, starting with members of the project Advisory Board. Each is interviewed, and those with specific experience in the effectiveness of mitigations are invited to a Zoom-based focus group process, supported by a new FGWare algorithm. After discussion to select a handful of CMs, each SME provides estimates of how much each specific mitigation reduces risk. We combine these estimates to form a consensus. We operationalize

"amount of risk reduction" based on Eq. 1, familiar throughout the field of risk management. The amount of risk reduction corresponds to the variable denoted by **E** in Eq. 2

$$R_0 = \text{Consequences} * \text{Vulnerability} * \text{Threat} \quad (1)$$

$$\text{Reduced Risk} = (1 - \mathbf{E}) * R_0 \quad (2)$$

We sketch the approach to two technical issues, detailed in [49].

To elicit probability distributions, as discussed in Section 1.2, we use a recent method aimed at experts unfamiliar with probabilities [50].

We ask each SME to sketch the probability density function, $\mathbf{E}(r, c)$, for each risk r and countermeasure c pair, (r, c). The expert moves colored dots successively, as in Figure 1, to set the median and range of the effectiveness, and, if desired, "fatten the tails." The underlying algorithm adjusts each side of the curve as a monomial. This supports both unimodal and bimodal estimates.

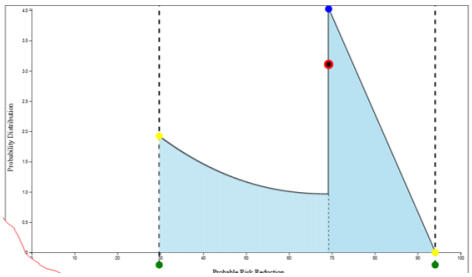

Figure 1. Five-point elicitation interface.

Individual estimates are aggregated by averaging and also by a generalization of [37] as discussed in Section 1.2. An example array of composite distributions is shown in Figure 2, in which an array of mean composite distributions is shown in green.

Clearly, the aggregate distribution is not "shoe-horned" into any particular parametric form. For example, it is clear that in the left column (counterfeit parts threat), the second CM (supplier vetting) is stronger than the first (careful examination of the parts) by almost any reasonable criterion. In the right-hand column (extreme weather threat) the second CM (diversify suppliers) is modestly to the right of the first (monitor weather forecasts). The scatter of the red dots signals the considerable disagreement among these experts in most cases. For simulation the **median** cumulated probability distributions are transmitted to the simulation team. The overall research plan is iterative, in the sense that when simulation or optimization sensitivity analysis calls for a sharper estimate for particular (r, c) pairs, we can return to selected experts and solicit additional data.

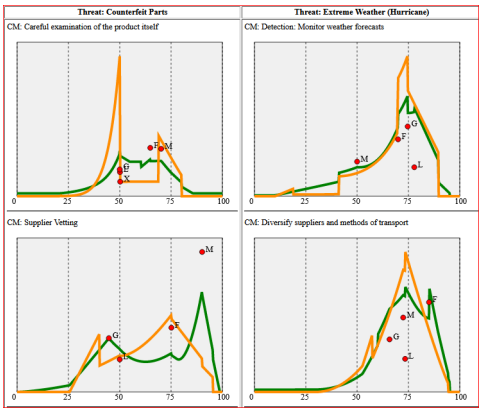

Figure 2. Array of aggregated expert opinions on density functions (see text).

3. Simulation

Assessing the resilience of a supply chain in terms of ability to "absorb" risk associated with disruptions and ability to "recover" its performance to pre-disruption is challenging. This may be accomplished by modeling the supply chain as a network where the nodes represent entities such as suppliers, manufacturing facilities, distribution centers (DCs) and customers while the arcs represent relationships among these entities and transportation links.

The anyLogistix software has been utilized to simulate supply chains with disruptions [51, 52, 53]. The simulation model in this paper is a discrete-event simulation model developed using the anyLogistix 2.13 software [2]. More information about the anyLogistix simulation environment can be found in [54].

3.1. Simulation model

In this section, a simulation model of an ICT supply chain network is developed under the natural hazards threat. Simulation models for our other two scenarios will be discussed in subsequent papers such as [55] so that we can describe our work on one of these scenarios in more detail here. Three CMs based on the results of the elicitation study (see Section 2) are investigated, and their effectiveness is assessed in simulation.

A simple yet realistic 4-stage ICT supply chain network as shown in Figure 3 illustrates the approach. It consists of three suppliers (S_1, S_2, and S_3, located in California, Florida, and Texas, respectively), two factories (F_1 and F_2), two DCs (DC_1 and DC_2) and n =100 customers ($C_1, C_2, ..., C_n$, randomly located in the US). All facilities in the network have their locations assigned, as shown in Figure 4.

The three suppliers together provide five different

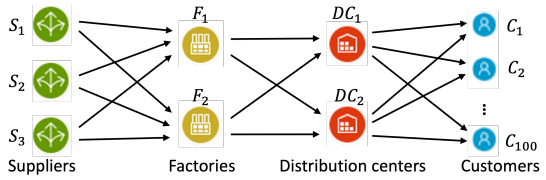

Figure 3. Supply chain network.

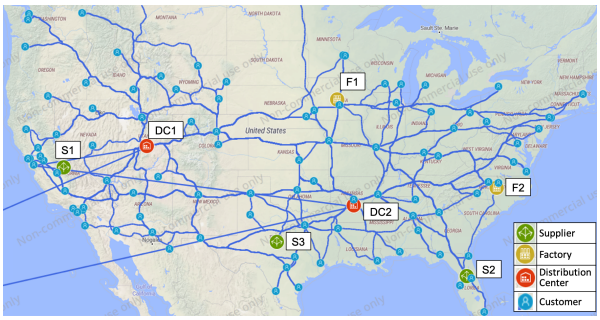

Figure 4. Simulated network of ICT supply chain.

components (screen, keyboard, motherboard, battery, and laptop base) to the factories. Factories assemble the components into laptops. Finished laptops are delivered to DCs and then customers.

3.1.1. Baseline scenario

In our baseline scenario, there are no disruptions to the supply chain, and its performance level is 100% (meeting all requested demand on time). Each of the five components is shipped from a supplier to a factory according to a pre-specified ratio. A factory may receive a type of component from one or more suppliers: S_1 provides a proportion p_1 of its demand, and similarly for S_2 and S_3. The values of (p_1, p_2, p_3) are shown in Table 1. For example, both factories receive all of their screens from S_1. F_2 receives 1/3 of the keyboards from S_1 and the remaining 2/3 from S_2. The transportation between a supplier and a factory takes 5 hours.

Table 1. Sourcing table showing proportions of components from each supplier to each factory.

(p_1, p_2, p_3)	F_1	F_2
Screen	(1, 0, 0)	(1, 0, 0)
Keyboard	(0.5, 0.5, 0)	(0.333, 0.667, 0)
Motherboard	(0, 0.625, 0.375)	(0, 0.333, 0.667)
Battery	(0, 1, 0)	(0, 0.167, 0.833)
Laptop base	(0, 0, 1)	(0, 0, 1)

Factories use the QR inventory policy (fixed replenishment quantity policy) with (Q, R) = (1000, 600), starting laptop inventory at s = 1500 units, and component inventory at r = 1000 units for each type. The throughput is p = 150 units/day at each factory. Each factory provides proportions of the demand to the DCs. DC_1's demand is fulfilled by F_1 and F_2 equally, while 40% of DC_2's demand is fulfilled by F_1 and 60% by F_2. The total factory demand is based on the requested demand from customers to the DCs. The transportation between a factory and a DC takes 5 hours.

DCs also use the QR policy with (Q, R) = (1000, 600) and starting inventory at s = 1500 units. Each of the customers places a demand every single day according to a uniform distribution of U(1, 3) units. The demand is sent to the closest DC. Based on the network in Figure 4, there are 45 customers sending orders to DC_1, and 55 customers to DC_2, every day. The transportation between a DC and a customer takes 3 days.

3.1.2. Threat scenario

In the threat scenario, natural hazards occur but no CMs are introduced. Factories F_1 and F_2 are located in an area subject to earthquakes and hurricanes respectively. When a natural hazard occurs, it will shut down the factory in the area for a number of days. The frequency of earthquakes/hurricanes and their severities are expressed by random variables based on the historical data of the area. The risk associated with the severity is the duration of the disruption, which is exaggerated from reality to better show the impact of the threat. Table 2 shows the parameters in this scenario.

Table 2. Model parameters in the threat scenario.

Natural hazard	**Earthquake**	**Hurricane**
Facility impacted	F_1	F_2
Frequency	Once during Jun-Nov	
Starting date	Random	
Duration (day)	60 w.p. 0.5, 90 w.p. 0.3, 120 w.p. 0.2	

3.1.3. Countermeasure scenarios

Three different CMs (CM1, CM2, and CM3) have been developed to provide resilience during disruptive events caused by natural hazards. CM1 and CM2 are reactive CMs that are implemented after the actual occurrence of the event. CM3 is a proactive CM designed for pre-disruption implementation.

When a factory is shut down due to a natural hazard, we can increase the throughput of the remaining operating factory to help meet the demand, but this increase takes several days to implement. So, in CM1, we increase the throughput of the remaining factory a few days after the disruption, and the throughput remains increased till the end of the disruption.

In CM2, we introduce an outsourcing factory to help cope with the demand. This outsourcing factory may be reconfigured and subcontracted to handle laptop

assembly, which takes several days. Since this factory is located in a non-impacted area, transportation between it and DCs takes longer.

Pre-disruption CM3 uses accurate monitoring systems for potential natural hazards, based on which early actions can be planned in advance. In the days leading to the disruption, we can increase the throughput of the to-be-impacted factory so that more laptops can be assembled before the event. The inventory policies of the DCs are adjusted accordingly so more finished laptops are delivered to DCs before the event.

Table 3 summarizes all five scenarios and the parameters in the three Threat + CM scenarios.

Table 3. Scenario description and parameters.

Scenario	Description
Baseline	Normal operation, no disruption.
Threat	Natural hazards occur but no CMs are introduced.
Threat + CM1	Ten days after disruption, the remaining operating factory's throughput increases to 200 units/day.
Threat + CM2	Ten days after disruption, an outsourcing factory becomes operational, but transportation from the outsourcing factory to DCs takes 10 days.
Threat + CM3	During the 15 days leading to disruption, factory's throughput increases to 200 units/day, and DC's reorder point increases to 900 units.

3.1.4. Performance metrics

Five performance metrics are computed to evaluate the performance of the supply chain and effectiveness of the CMs.

(1) **ELT Service Level by Orders** shows the service level based on the ratio of on time orders to the overall number of outgoing orders:

$$ELTSL^{(i)} = OTO/(OTO + DO) \tag{3}$$

where i is the facility index, OTO is the number of on time orders, and DO is the number of delayed orders. $OTO + DO$ is the number of outgoing orders. The ELT (expected lead time) is set at 4 days, allowing 3 days for transportation and 1 day for order processing. An on time order is one for which the time from customer order placement to delivery is within the ELT.

(2) **Service Level by Orders** shows the service level based on the ratio of the number of successfully fulfilled orders to the sum of all orders placed for this facility:

$$SL^{(i)} = SO/(SO + UO) \tag{4}$$

where i is the facility index, SO is the number of orders that are successfully fulfilled, and UO is the number of unsuccessful orders. Unsuccessful orders are the placed orders requiring the quantity of products that is not available at the facility at the time of order placement.

(3) **Max Lead Time** is the maximum time between order placement and delivery across all orders.

(4) **Mean Lead Time** is the average time between order placement and delivery across all orders.

(5) **Fulfillment (Late Products)** shows the quantity of product which fails to arrive within the specified ELT.

3.2. Results and comparison

We use feedback from stakeholders (industry Advisory Board and DHS) throughout network model design and simulation to verify the work by using small-size, deterministic demand and following it through the network using "manual" calculations. After the verification process, the demand is increased and more stochasticity added, and we simulate for one year to observe enough inventory cycles and stockout situations, with 30 replications per scenario. The number of replications is chosen for the Central Limit Theorem to hold. The 30 replications take about 60 seconds on a Windows 2017 computer (Intel Core i7). Model validation is achieved by discussing the output with the stakeholders, but true validation will only be possible when/if the model is used by government or industry in specific situations.

The *ELT service level by orders* and *service level by orders* are recorded for each day in the simulation. The daily values are then averaged over the threat period within each replication. Table 4 shows the "threat period average" values across 30 replications. A service level closer to 1 indicates a more resilient supply chain. As can be seen, both metrics are severely affected when no CMs are employed. All 3 CMs improve upon the threat scenario. CM2 is the least effective one, because it is enacted 10 days after the threat has occurred and the transportation time from the outsourcing factory is 7 days more than usual. This is why the ELT service level is still poor. CM1 is ranked second. This CM is also enacted 10 days after the threat has occurred but the production speed of the remaining factory is increased with no extra transportation time. CM3 is the most effective CM due to the 15-day early actions obtained and the increased inventory levels and production speeds to deal with the threat.

Table 4. Average service levels from simulation.

	ELT Service Level		Service Level	
Scenario	DC_1	DC_2	DC_1	DC_2
Threat only	0.3762	0.3678	0.3276	0.3292
Threat + CM1	0.9616	0.9272	0.9675	0.9549
Threat + CM2	0.8089	0.7947	0.7917	0.7668
Threat + CM3	0.9985	0.9955	0.9970	0.9944

The max lead time and mean lead time performance metrics are summarized in Table 5, showing the average

values across 30 replications. The lead time from DC to customer is 3 days in the baseline scenario. CM3 is still the most effective CM based on both metrics, closely followed by CM1, and then CM2. While CM2 improves the lead times from the threat scenario, the lead times are higher because of extra transportation time from the outsourcing factory. CM3 results in the lowest lead times, which are only slightly higher than those in the baseline. CM1 results in slightly higher max lead times than CM3, and mean lead times comparable with CM3.

CM1 and CM3 are comparable when looking at service levels and lead times, but the difference between CM1 and CM3 is more evident in the fulfillment metric. The average values are shown in the rightmost section of Table 5. The average fulfillment of late products at DC_2 is lower in CM3 than in CM1, making CM3 more effective than CM1.

Table 5. Average lead times and fulfillment

	Max Lead Time		Mean Lead Time		Fulfillment	
Scenario	DC_1	DC_2	DC_1	DC_2	DC_1	DC_2
Baseline	3.00	3.00	3.00	3.00	-	-
Threat only	42.79	45.87	13.32	15.52	57.22	69.78
Threat + CM1	5.91	6.78	3.04	3.05	3.11	4.22
Threat + CM2	12.72	14.36	4.76	5.17	25.64	22.57
Threat + CM3	3.36	3.54	3.01	3.01	3.89	1.83

These results show the effectiveness in terms of performance metrics of the CMs for mitigating the impact of natural hazards in the ICT supply chain. CM3 is seen to be the most effective, most likely because of the planned early actions. When early warnings are not available, CM1 with increased throughput of the remaining factory would be the next best option.

4. Optimization

In general, a set of several CMs can be proposed to mitigate the impact of natural hazards considered in Section 3. A CM might be proactive as CM3 or reactive as CM1 and CM2. Different variants of a CM might be considered, e.g., increase production 5 days or 10 days before a forecast hurricane. Since the natural disasters are described by random variables, the ameliorative effect of any given CM must be evaluated by simulation runs. If only a single optimal CM can be chosen according to some performance measures, methods of Section 3 apply. When multiple CMs can be chosen, the combinatorial explosion of possibilities requires a stochastic optimization approach.

The two major classic approaches to stochastic optimization are chance-constrained programming, which models the assumption that a constraint holds $100(1-\epsilon)\%$ of the time for some small ϵ, and multi-stage programming, in which decisions on the variables are made at two or more points in time [56]. However, these approaches provide a single solution, whereas in practice decision makers want insight, and not just the output of an optimization tool [57]. In particular, we want to present the decision maker with different strategies, and a quantitative assessment of how often each strategy is optimal, depending on the realizations of the random variables. Thus we solve a sequence of optimization problems, where each problem uses the data of a single replication of the anyLogistix simulation model developed in Section 3. The problem defined by a single replication is fed to an optimization tool that solves an integer program to select the optimal set of CMs, subject to a budget constraint. This optimal set of CMs is stored. Then another replication is generated by anyLogistix, the associated data is sent to the optimization tool, the new optimal set of CMs is stored, and this process continues for the desired number of anyLogistix replications. These optimal sets of CMs (there is one set for each replication) are then analyzed, using some predefined decision rule, to determine which optimal set of CMs should be implemented.

4.1. Mathematical Formulation

We consider the demand for a single product by customers in each of T time periods, e.g., a day or a week. (Future work will consider a final product composed of many components, e.g., the laptop example in Section 3.) Let $\mathcal{J}$ be the set of customers, and for $j \in \mathcal{J}$ and $t \in \mathcal{T} \equiv \{1, 2, \cdots, T\}$, let $d(j,t)$ be the demand for the product by customer j in period t; we assume each $d(j,t)$ is a random variable with a given distribution. The product is produced by factories in a supply chain: factories feed finished product to DCs, and DCs feed the finished product to customers. Each factory can supply multiple DCs. For each factory, the fraction of its output going to each DC is specified. Each DC supplies multiple customers, and each customer is served by a specified DC. Figure 5 illustrates this for a simpler system with two factories, two DCs, four customers, and four time periods ($T = 4$). Each 4-tuple represents the demand or supply for product in each time period, e.g., for customer $R1$ the demand in the 4 time periods is $(3, 1, 6, 5)$ and the production level of factory $F1$ in the 4 time periods is $(4, 6, 4, 6)$.

Let N be the number of CMs and let $\mathcal{N} \equiv \{1, 2, \cdots, N\}$. CM $n \in \mathcal{N}$ is specified by a vector $v(n)$ of length T, generated by simulation, which provides the amount of product provided by the CM in each time period. For example, if $T = 7$, then for some $n \in \mathcal{N}$ we might have $v(n) = (0, 8, 9, 9, 6, 4, 0)$, meaning that n supplies 0 units at $t = 1$, 8 units at $t = 2$, etc. Also

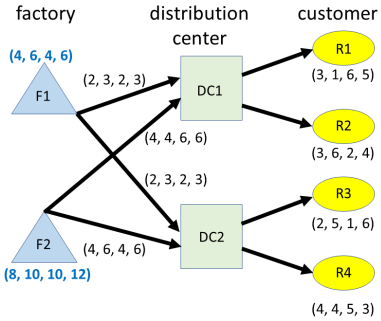

Figure 5. Example supply chain with $T = 4$.

associated with n is a cost $cost(n)$ e.g., a fixed cost of opening an emergency assembly site plus an incremental cost for each unit produced at the site over the T time periods. For $n \in \mathcal{N}$, let the binary variable $x(n)$ be defined by $x(n) = 1$ if CM n is implemented, and $x(n) = 0$ otherwise. A budget B limits the total cost of CMs: $\sum_{n\in\mathcal{N}} cost(n)x(n) \leq B$. Each factory sends its output to one or more DCs, and the fraction of the output of a given factory to the set of DCs is given data. Since CMs offset the loss in production capacity at a specific factory when disasters occur, the output of each CM is allocated to the set of DCs using these same fractional allocations. Let $\mathcal{DC}$ be the set of DCs.

If a threat materializes, and the factories are unable to ship sufficient products to meet the demand for one or more customers, demand is backlogged rather than lost. The objective is to minimize the total (over all time periods and customers) backlogged demand. Since each customer is served by a particular DC i, for each time period t we can sum (over all customers) the demand to be served by DC i; let $d(i,t)$ be this aggregate demand at DC i in period t. Let $s(i,t)$ be the amount of product supplied to DC i at time t given the current replication. For example, if the replication has no threat occurring, then $s(i,t)$ is the amount supplied to DC i under normal operating conditions, while if the replication has reduced production at one or more factories, then $s(i,t)$ reflects the reduced product available at DC i at time period t if no CM is implemented. For a given t the amount of backlogged demand at DC i if no CM is implemented is $\max\{d(i,t) - s(i,t), 0\}$.

For $n \in \mathcal{N}$ and $i \in \mathcal{DC}$ and $t \in \mathcal{T}$, let $b(n,i,t)$ be the given data specifying the amount of product provided at time t to DC i if CM n is implemented. If CM n does not back up DC i then $b(n,i,t) = 0$. Then the total threat mitigation supply sent by all CMs to DC i in time t is $\sum_{n\in\mathcal{N}} b(n,i,t)x(n)$, the total amount $L(i,t)$ of product backlogged at DC i at time t is

$$L(i,t) \equiv max\Big\{d(i,t) - s(i,t) - \sum_{n\in\mathcal{N}} b(n,i,t)x(n), 0\Big\}$$

and the total amount of product backlogged over all DCs and over all time periods is the objective function $F(x)$:

$$F(x) \equiv \sum_{t\in\mathcal{T}} \sum_{i\in\mathcal{DC}} L(i,t)\,.$$

Using standard techniques for dealing with a "max" term, $F(x)$ can be converted to a linear objective function together with associated constraints. The Python PuLP package [58], using the COIN-OR CBC solver [59], solves the optimization problem. The solution to this optimization problem (corresponding to a particular simulation replication) is stored, and another simulation replication is generated. Together they support calculations of the mean impact and other measures of risk and resilience.

The results of the optimization expand upon the conclusions in Section 3 that CM3 is the most effective CM, followed by CM1, and then CM2. With 100 replications and $B = 1$, CM3 at factory 1 (F1) is chosen 69 times, and CM3 at F1 is chosen 31 times. With 100 replications and $B = 2$, CM3 at both F1 and F2 is chosen 100 times. We also studied a larger example, with 8 factories, 6 distribution centers, 100 customers, and $B = 2$. With 100 replications, 18 distinct sets of CMs were generated; the most frequent set generated (25 replications) used CM3 at F2 and F4; the next most frequent set (19 replications) used CM3 at F2 and F3.

5. Discussion

This work models an end-to-end approach that recognizes the fundamentally stochastic nature of risk mitigation and resilience. By developing the three components of elicitation, simulation, and optimization we are able to inform each component by the specific and changing needs of the other two, which brings us closer to the goal of providing a sound quantitative methodology for making rational decisions under a limited budget for risk mitigation.

If either simulation or optimization should reveal that the conclusions are particularly sensitive to the details of a distribution describing some risk-mitigation CM, SMEs could be reconvened to look for a resolution.

The integrated approach presented here offers specific operationalizations of the concepts of uncertainty about the effectiveness of mitigations, and the stochastic nature of all threats. The framework permits comparison of CMs not solely in terms of costs, but also in terms of their likely ability to control associated risks. With suitable choices of the objectives and performance metrics, this technology can be adapted for use at a single plant, a multi-location organization, or a state or federal agency.

There are numerous opportunities to enhance the optimization model described in Section 4. The software could accept a CM scenario and automatically generate variations of it, or could be enhanced to consider the impact of the QR inventory policies described in Section 3.1.1 or to allow any of the performance metrics described in Section 3.1.4 to be used as the objective function of the optimization.

Crucial information on effectiveness of specific CMs is gained in painful experience such as business setback or failures. Organizations are unwilling to share such information; even when resilience is achieved, that fact may well be regarded as a proprietary advantage. A somewhat similar problem exists in the airline industry. However, over the years the commercial airlines and the Federal Aviation Administration have developed a secure and trusted system for reporting not only accidents, but also the much more common "near misses." This work contributes toward a similar trust and benefit for the ICT supply chain. By a systematic integration of elicitation, simulation, and optimization, our work provides a unified framework to assess CM effectiveness, strengthen resilience, and support planning and decision-making.

6. Acknowledgments

Acknowledgement: This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 17STQAC00001-05-00. **Disclaimer:** The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security. The authors thank Niles Egan and Vladimir Menkov for construction of the 5-point elicitation tool.

References

[1] CISA Working Group 2, "INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE Threat Evaluation Working Group: Threat Scenarios Version 2.0." https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v2.pdf, 2021.

[2] The AnyLogic Company, "anyLogistix supply chain optimization software." https://www.anylogistix.com, 2021.

[3] K. Katsaliaki, P. Galetsi, and S. Kumar, "Supply chain disruptions and resilience: a major review and future research agenda," *Ann. Oper. Res.*, pp. 1–38, 2021.

[4] B. Fahimnia, C. S. Tang, H. Davarzani, and J. Sarkis, "Quantitative models for managing supply chain risks: A review," *Eur. J. Oper. Res.*, vol. 247, pp. 1–15, 2015.

[5] C. W. Craighead, J. Blackhurst, M. J. Rungtusanatham, and R. B. Handfield, "The severity of supply chain disruptions: design characteristics and mitigation capabilities," *Decision Sci.*, vol. 38, pp. 131–156, 2007.

[6] Centre for Research on the Epidemiology of Disasters, "EM-DAT: The International Disaster Database." https://www.emdat.be/.

[7] D. Gama Dessavre, J. E. Ramirez-Marquez, and K. Barker, "Multidimensional approach to complex system resilience analysis," *Reliab. Eng. Syst. Safe.*, vol. 149, no. C, pp. 34–43, 2016.

[8] Y. Li and C. W. Zobel, "Exploring supply chain network resilience in the presence of the ripple effect," *Int. J. Prod. Econ.*, vol. 228, p. 107693, 2020.

[9] M. Ouyang and L. Dueñas Osorio, "Time-dependent resilience assessment and improvement of urban infrastructure systems," *Chaos*, vol. 22, p. 033122, 2012.

[10] C. Zobel and L. Khamsa, "Characterizing multi-event disaster resilience," *Comput. Oper. Res.*, vol. 42, pp. 83–94, 2014.

[11] GIDEP, "About GIDEP." https://www.gidep.org/about/about.htm.

[12] ERAI, "About ERAI, Inc.." https://www.erai.com/aboutus_profile.

[13] *Counterfeit Material Process Guidebook: Guidelines for Mitigating the Risk of Counterfeit Materiel in the Supply Chain*. NAVSO P-7000: Office of the Assistant Secretary of the Navy (Research, Development & Acquisition) Acquisition and Business Management, 2017-06.

[14] S. Wix and D. Mahadeo, "Suspect/counterfeit electronics overview," *Component & System Analysis*, 2017-05-11.

[15] A. R. Szakal and K. J. Pearsall, "Open industry standards for mitigating risks to global supply chains," *IBM J. RES. & DEV*, vol. 58, no. 1, p. 1:1–13.

[16] C. Metz, *Counterfeit Items Detection and Prevention*. DLA J-334,: Defense Logistics Agency, America's Combat Logistics Support Agency, 2012-09.

[17] J. S. Gansler, W. Lucyshyn, and J. Rigilano, *Addressing counterfeit parts in the DOD supply chain*. UMD-LM-14-012: Center for Public Policy and Private Enterprise, School of Public Policy, University of Maryland, 2014-03.

[18] Lockheed Martin, "Counterfeit prevention: What makes a good control plan?." https://slidetodoc.com/counterfeit-prevention-what-makes-a-good-control-plan/.

[19] D. A. Bodner, "Enterprise modeling framework for counterfeit parts in defense systems," *Procedia Computer Science*, vol. 36, pp. 425–431.

[20] R. A. Martin, "Trusting our supply chains: A comprehensive data-driven approach," tech. rep., MITRE Center for Data-Driven Policy, 2021-01 https://www.mitre.org/sites/default/files/publications/pr-20-01465-37-trusting-our-supply-chains-a-comprehensive-data-driven-approach.pdf.

[21] DARPA, "A DARPA approach to trusted microelectronics." https://www.darpa.mil/attachments/ObscurationandmarkingSummary.pdf.

[22] R. Lingle, "In-mold labels use digital watermarking for authentication," *Packing Digest*, 2014-11-26, https://www.packagingdigest.com/trends-issues/mold-labels-use-digital-watermarking-authentication.

[23] Digital Watermarking Alliance, "Authentication of content and objects (includes government ids)." https://digitalwatermarkingalliance.org/digital-watermarking-applications/authentication-of-content-and-objects/.

[24] CDC, "Tamper-resistant prescription form requirements." https://www.cdc.gov/phlp/docs/menu-prescriptionform.pdf.

[25] M. Chen, F. Brun, M. Raynal, C. Debord, and D. Makowski, "Use of probabilistic expert elicitation for assessing risk of appearance of grape downy mildew," *Crop Protection*, vol. 126, p. 104926, Dec. 2019.

[26] N. C. Dalkey, "The Delphi Method: An experimental study of group opinion," RAND Corporation Report RM-5888-PR, 1969.

[27] H. A. Linstone and M. Turoff, eds., *The Delphi Method: Techniques and Application*. Reading, MA: Addison Wesley, 1975.

[28] W. P. Aspinall and R. M. Cooke, "Quantifying scientific uncertainty from expert judgement elicitation," in *Risk and Uncertainty Assessment for Natural Hazards* (J. Rougier, S. Sparks, and L. Hill, eds.), Cambridge University Press, 2013.

[29] S. Mitchell and I. Dunning, "MATCH Elicitation tool." http://optics.eee.nottingham.ac.uk/match/uncertainty.php#, 2021.

[30] D. E. Morris, J. E. Oakley, and J. A. Crowe, "A web-based tool for eliciting probability distributions from experts," *Environ. Modell. Softw.*, vol. 52, pp. 1–4, 2014.

[31] P. B. Kantor, "Soft triangles for expert aggregation," *arXiv preprint arXiv:1909.01801*, 2019.

[32] R. T. Clemen and R. L. Winkler, "Combining probability distributions from experts in risk analysis," *Risk Anal.*, vol. 19, no. 2, pp. 187–203, 1999.

[33] W. G. Stillwell, D. V. Winterfeldt, and R. S. John, "Comparing hierarchical and non-hierarchical weighting methods for eliciting multiattribute value models," *Manage. Sci.*, vol. 33, pp. 442–450, 1987.

[34] E. J. Bonano, S. Hora, R. Keeney, and D. Von Winterfeldt, "Elicitation and use of expert judgment in performance assessment for high-level radioactive waste repositories," tech. rep., Nuclear Regulatory Commission, 1990, doi:10.2172/6842967.

[35] R. L. Keeney and D. Von Winterfeldt, "Eliciting probabilities from experts in complex technical problems," *IEEE T. Eng. Manage.*, vol. 38, pp. 191–201.

[36] S. C. Hora, "Eliciting probabilities from experts," in *Advances in Decision Analysis: From Foundations to Applications* (W. Edwards, R. Miles Jr., and D. Winterfeldt, eds.), Chapter 8: Cambridge University Press, 2007.

[37] F. Y. Edgeworth, "On observations relating to several quantities," *Hermathena*, vol. 6, pp. 279–285, 1887.

[38] W. Ho, T. Zheng, H. Yildiz, and S. Talluri, "Supply chain risk management: A literature review," *Int. J. Prod. Res.*, vol. 53, no. 16, pp. 5031–5069, 2015, doi:10.1080/.

[39] D. White, "Application of systems thinking to risk management: A review of the literature," *Manage. Decis.*, vol. 33, no. 10, pp. 35–45, 1995.

[40] F. Benaben, L. Faugere, B. Montreuil, M. Lauras, N. Moradkhani, T. Cerabona, J. Gou, and W. Mu, "Instability is the norm! a physics-based theory to navigate among risks and opportunities," *Enterprise Information Systems*, pp. 1–28, 2021.

[41] P. Edwards and P. Bowen, *Risk Management in Project Organisations*. Oxford, UK: Elsevier, 2005.

[42] R. Kumar, L. Ganapathy, R. Gokhale, and M. K. Tiwari, "Quantitative approaches for the integration of production and distribution planning in the supply chain: a systematic literature review," *Int. J. Prod. Res.*, vol. 58, no. 11, pp. 3527–3553, 2020.

[43] D. Ivanov and A. Dolgui, "A digital supply chain twin for managing the disruption risks and resilience in the era of industry 4.0," *Prod. Plan. Control.*, pp. 1–14, 2020.

[44] J. Olivares-Aguila and W. ElMaraghy, "System dynamics modelling for supply chain disruptions," *Int. J. Prod. Res.*, vol. 59, no. 6, pp. 1757–1775, 2021.

[45] C. Thierry, A. Thomas, and G. Bel, "Simulation for supply chain management: An overview," *ISTE Ltd and John Wiley and Sons Inc*, 2008.

[46] M. Jahangirian, T. Eldabi, A. Naseer, L. K. Stergioulas, and T. Young, "Simulation in manufacturing and business: A review," *Eur. J. Oper. Res.*, vol. 203, no. 1, pp. 1–13, 2010.

[47] J. B. Oliveira, R. S. Lima, and J. A. B. Montevechi, "Perspectives and relationships in supply chain simulation: A systematic literature review," *Simulation Modelling Practice and Theory*, vol. 62, pp. 166–191, 2016.

[48] E. A. Elsayed, *Reliability Engineering*. John Wiley & Sons, 2012.

[49] N. Egan, V. Menkov, and P. Kantor, "Eliciting Uncertain Resilience Information for Risk Mitigation," *HICSS*, 2022 (to appear).

[50] Author. *Details omitted to preserve blind review*.

[51] G. Timperio, S. Tiwari, J. M. Gaspar Sánchez, R. A. García Martín, and R. De Souza, "Integrated decision support framework for distribution network design," *Int. J. Prod. Res.*, vol. 58, no. 8, pp. 2490–2509, 2020.

[52] A. Kinra, D. Ivanov, A. Das, and A. Dolgui, "Ripple effect quantification by supplier risk exposure assessment," *Int. J. Prod. Res.*, vol. 58, no. 18, pp. 5559–5578, 2020.

[53] S. Singh, R. Kumar, R. Panchal, and M. K. Tiwari, "Impact of COVID-19 on logistics systems and disruptions in food supply chain," *Int. J. Prod. Res.*, vol. 59, no. 7, pp. 1993–2008, 2021.

[54] D. Ivanov, "Supply chain simulation and optimization with anyLogistix," *Berlín School of Economics and Law, Germany*, 2018.

[55] R. Lei, S. Saleh, W. Guo, E. A. Elsayed, P. Kantor, E. Rosenberg, and F. Roberts, "Modeling ICT supply chains under threat of counterfeit parts," *manuscript in preparation*.

[56] F. Hillier and G. Lieberman, *Introduction to Mathematical Programming*. McGraw Hill, 1990.

[57] A. Geoffrion, "The purpose of mathematical programming is insight, not numbers," *Interfaces*, vol. 7, pp. 81–92, 1976.

[58] I. Stuart Mitchell, "Pulp: A linear programming toolkit for python." https://pypi.org/project/PuLP/.

[59] COIN-OR Foundation, "Cbc." https://projects.coin-or.org/Cbc.