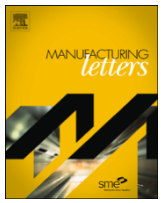
Available online at www.sciencedirect.com

Manufacturing Letters

Manufacturing Letters 00 (2023) 000–000



51st SME North American Manufacturing Research Conference (NAMRC 51, 2023)

Simulation modeling of the counterfeit threat and countermeasures in ICT manufacturing supply chains

Rong Lei[a], Samar Saleh[a], Weihong "Grace" Guo[a,*], Elsayed A. Elsayed[a], and Fred S. Roberts[b]

[a] *Department of Industrial and System Engineering, Rutgers University-New Brunswick, Piscataway, NJ 08854, USA*
[b] *CCICADA Center and Department of Mathematics, Rutgers University-New Brunswick, Piscataway, NJ 08854, USA*

* Corresponding author. Tel.: +1-848-445-8556. *E-mail address:* wg152@soe.rutgers.edu

Abstract

There has been great concern about building resilient supply chains to expedite the supply chain's recovery after a crisis or disruption. Few attempts, however, were made to study the resiliency of a supply chain after disruptions caused by counterfeit parts, especially in critical domains like information and communication that are embedded in almost every aspect of our daily lives and critical life-supporting systems. Counterfeits will penetrate a supply chain at one of the suppliers' or manufacturers' points. Hence, rigorous countermeasures should be taken at these stages. Using a hybrid simulation model, this paper studies the performance of an Information and Communication Technology (ICT) manufacturing supply chain subject to counterfeit parts risks and specific countermeasures. The system's service levels, delivery time, and proportion of good products are the performance measures adopted to determine the effectiveness of the countermeasures and thus the supply chain resiliency. The model can be extended to other types of supply chain networks and help manufacturers adopt the optimum countermeasures.

© 2023 Society of Manufacturing Engineers (SME). Published by Elsevier Ltd. All rights reserved.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Peer-review under responsibility of the Scientific Committee of the NAMRI/SME.
Keywords: Counterfeit; manufacturing supply chain; risk analysis; resilience; Information and communication technology (ICT)

1. Introduction

1.1. Motivation

A legitimate business suffers financial losses each time a purchase of a counterfeit good takes place. This eventually leads to lost earnings and jobs. Counterfeiting, called "perhaps the world's fastest growing and most profitable business" by the Business Week magazine in 1985 [1], continues to evolve and haunts every business sector. Counterfeit parts include apparel, software, pharmaceuticals, electronics, and components used to make other things like auto parts, aviation parts, electronic parts, etc. The Society of Automotive Engineers defines counterfeit as "A fraudulent part that has been confirmed to be a copy, imitation, or substitute that has been represented, identified, or marked as genuine, and/or altered by a source without legal right with intent to mislead, deceive, or defraud [2]." The Department of Defense (DoD) limited counterfeits to electronic counterfeits in its definition in 2014 [3, 4].

A report by Frontier Economics for the International Chamber of Commerce and The International Trademark Association estimates that international trade, local manufacturing, and consumption of counterfeit pirated goods were $917 billion in 2013 and are anticipated to reach $1.5-1.9 trillion in 2022. Counterfeiting also causes job turnover, estimated between 2.0-2.6 million in 2013 and 4.2-5.4 million by 2022 [5]. This multi-billion market, which accounts for 3.3% of worldwide commerce and shows an 80% increase in only five years (from 2008 to 2013) [6], is of importance to corporations because of its impact on sales, firm reputation, and brand value. Many organizations and countries attempt to resist its spread due to its detrimental influence on innovation, economy, citizen welfare and

2213-8463 © 2023 Society of Manufacturing Engineers (SME). Published by Elsevier Ltd. All rights reserved.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Peer-review under responsibility of the Scientific Committee of the NAMRI/SME.

safety, and the ability to be involved in criminal networks and organized malignant groups that destabilize society.

We've seen a rise in counterfeit items due to e-commerce which makes counterfeits harder to track and the Covid-19 pandemic which limited suppliers due to rigorous onboarding regulations. Some countries' reluctance to send electronic debris to underdeveloped countries drives "e-waste recycling," which is recycled, re-labeled, and sold as genuine. Technological advances help counterfeiters make cheaper, harder-to-detect fakes. To minimize costs, corporations turn to suppliers in countries with fewer regulations. Counterfeiters hide in long, complicated supply chains (SCs), where counterfeits are hard to trace. A counterfeit part may be processed through many subsystems in an SC before entering the final product. Here, it's on to manufacturers at all levels to implement anti-counterfeiting measures and reduce the vulnerability of the SC.

1.2. Objective

Counterfeiting has been studied for decades. In most circumstances, a system failure causes a root cause failure analysis that fails to uncover that a counterfeit part caused the breakdown. Sometimes linked to damaged components during assembly or use which impair a company's reliability and sales. To avert this, researchers, manufacturers, business coalitions, and certain governments tried to stop counterfeits from reaching the final consumer or product.

There are two ways to reduce counterfeits in the supply chain. The first intends to limit the likelihood of this disruption by utilizing detection and authentication mechanisms for supplied parts at each tier. The second type builds a resilient supply chain to limit disruption's effects. The two tactics differ in techniques, procedures, and accountable party, but can work together to build a less-vulnerable SC. This study models a typical ICT (Information and Communication Technology) manufacturing SC disrupted by counterfeit parts if backed by anti-counterfeiting measures. The SC's resilience is tested using multiple performance metrics.

1.3. Literature review

Strong attempts continuously evolve to immune firms against counterfeits. Detection methods and product authentication are the first defense barrier. Several types of counterfeits exist and the dominant types of counterfeits threatening today's SCs are recycled and remarked on. Recycled counterfeits are things the legitimate manufacturer discards after performance degradation or aging, then a counterfeiter sells. The counterfeits are either scraped or actual new products remarked as improved. Guin *et al.* [7, 8] outline counterfeit component tests in Fig. 1. Methods of counterfeit detection are effective and evolving, but there is no effective solution because each test is effective for certain types of counterfeits and an SC can be attacked by different types. While buying from authorized wholesalers is always recommended, the U.S. Department of Commerce reports that even authorized distributors face counterfeits [9].

Supply chain partners, including manufacturers, should identify counterfeit breakthrough points and secure them using the aforementioned detection methods. Besides testing,

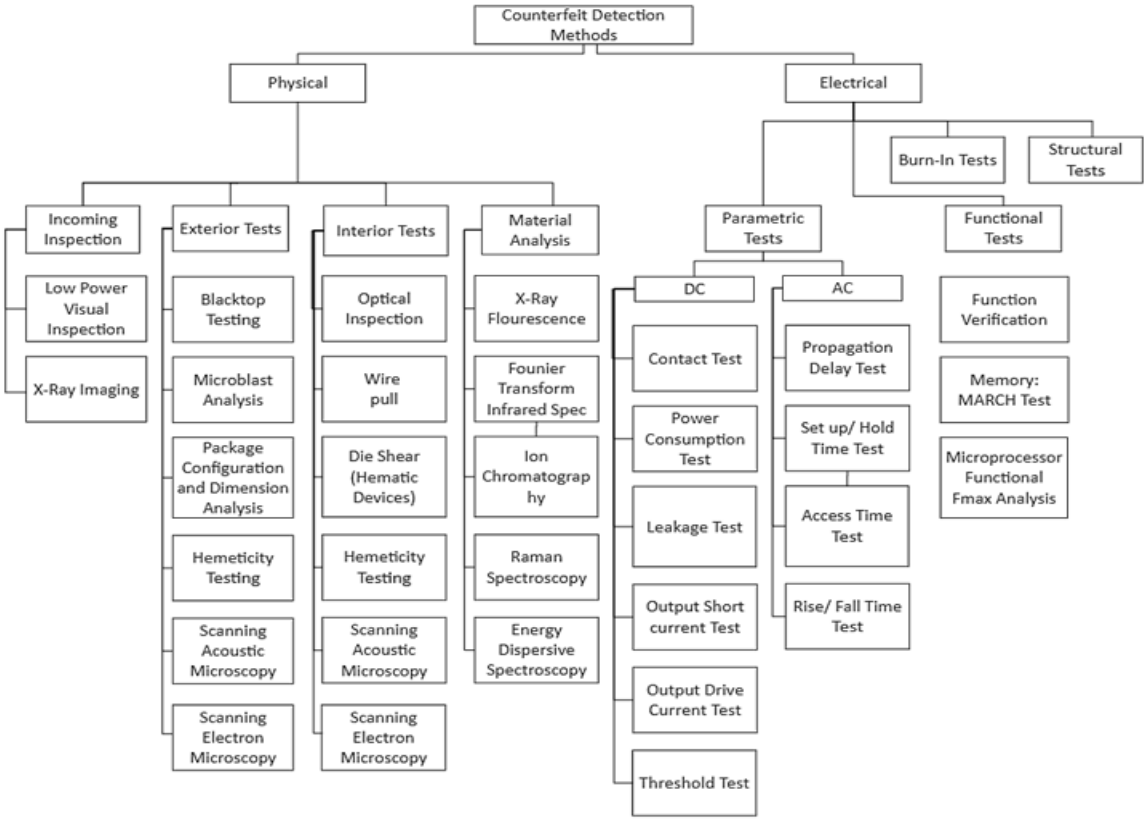


Fig. 1. Taxonomy of Counterfeit Detection [7].

anti-counterfeiting technologies include functions such as authentication, tracking/tracing, and anti-tampering/anti-alteration. Anti-counterfeiting technologies include electronic, marking, chemical and physical, mechanical, and digital media technologies with blockchain [10].

Technologies detailed in Table 1 range in uses, costs, and implementation, but they have one common characteristic: connecting marking devices into products. Some researchers added self-validation so customers can check the product's validity using their phones [11, 12]. Knowing that these preventative measures aren't 100% effective and are utilized pre-disruption, an SC should use mitigation techniques to control disruptions and their consequences.

As mentioned earlier, building a resilient supply chain (SCRES) is another way to reduce counterfeits. In 2005, a study found that companies unprepared for disruptions had 30% lower shareholder returns [13]. SCRES is the ability to proactively plan and design the supply chain network for anticipating unexpected disruptive events, responding adaptively to disruptions while maintaining control over structure and function, and transcending to a post-disruption, robust state of operations, if possible, a more favorable one than before the event [14]. Scholars and stakeholders are directing their intentions and investments toward SCRES to reduce the impact of a disruption, obtain a competitive edge, and improve market position. Soni *et al.* [15, 16] use graph theory to explain SCRES enablers and interactions and compute a resilient index to quantify resilience, guiding enterprises to create the most resilient SC based on its enablers.

SC disruptions can be caused by several factors. Oke and Gopalakrishnan [17] describe risk mitigation measures after categorizing all hazards into supply, demand, and miscellaneous. Snyder *et al.* review the research to model natural or human disturbances while developing a new SC [18] or fortifying an existing one [19].

Despite the range of researched disruptions, none tackles SC disruptions related to counterfeits or builds a model to analyze SC robustness while adopting countermeasures. Ghadge *et al.* [20] highlight that and describe the current situation of counterfeiting in ICT manufacturing SC, including the most successful anti-counterfeiting tactics, based on experts' experience. The best strategies were beyond-second-tier network visibility, pre-supply appraisal, and high-level specifications and supplier relationships.

Simulation models can turn Ghadge *et al.*'s [20] theoretical explanation into quantitative models to forecast the effects of counterfeits and the effectiveness of countermeasures and enable validated anti-counterfeiting decision-making. Some studies concur that counterfeits will enter the SC despite rigorous countermeasures; for example, a hostile insider can circumvent them [21]. Traceability is proposed to prevent counterfeit parts from entering the electrical, electronic, and electromechanical supply chain. Without quality control, traceability is ineffective [22]. Etemadi *et al.* [23] support blockchain as an innovative method for preventing disturbances to cyber SC.

Contrary to refs. [22] and [23], counterfeits cannot be combated by focusing simply on the part because the ICT manufacturing supply chain is vulnerable to counterfeiters. Mani *et al.* [24] describe three important supply chain points that create counterfeit risk (manufacturer, distributor, and customer). The paper investigates counterfeit risks in the field programmable gate array and models the impact of mitigation methods for each driver. Flexibility in distribution, part lead time management, and information exchange with downstream partners are suggested. Gossena *et al.* [25] offer a way to analyze counterfeit risk scenarios and quantify the likelihood of a successful attack and the effectiveness of proposed defenses. DOD's work combating counterfeit materials is groundbreaking. It establishes investigating, preventing, detecting, and responding guidance to counterfeits. DOD's Systems Engineering Research Center investigates the cost and impact of enacting anti-counterfeiting policies on the enterprise utilizing an enterprise modeling framework [26, 27].

In previous research about counterfeits countermeasures, essential performance criteria, such as the firm's service level and proportion of good products, were not analyzed. Using simulation to obtain quantitative performance outcomes after adopting countermeasures will convince decision-makers who distrust countermeasures and dread investing in them despite the mounting threat of counterfeits. In our study, we develop a hybrid simulation model to analyze a laptop manufacturer's performance when faced with counterfeit threats. The simulation parameters are determined by experts from different fields. The focus is on counterfeit motherboards because they are key to laptop functionality. The performance is measured by the firm's service level, delivery time, and proportion of good parts.

The remainder of this paper is organized as follows: Section 2 explains the simulation model created to analyze

Table 1. Anti-counterfeiting technologies [10].

Type	Anti-counterfeiting technologies
Electronic	- RFID (Radio Frequency Identification) - NFC (Near field Communication) - Electronic Seals - Magnetic Stripes - Contact Chips
Marking	- Optical Memory Stripe - Machine Readable Codes - Unique Identifier Marks - Microtexts - Guilloche/ Rainbow Printing - Encrypted Images - Watermarks - Inks - Holograms
Chemical & physical	- DNA Coding - Glue Coding - Surface Fingerprint - Chemical Encoding and Tracers
Mechanical	- Labels - Laser Engraving - Anti-Alteration Devices - Security Threads - Security Film
Digital media technologies	- Digital Rights Management Systems - Digital Watermarks - Hashing - Fingerprinting - Seals
Shared ledger	- Block-chain

supply chain network performance in three scenarios with three different countermeasures. Section 3 discusses results and findings. Section 4 provides concluding remarks and discusses future research directions.

2. Method

In this section, a simulation model of an ICT manufacturing supply chain network is created to analyze different scenarios of counterfeit threats. The model is developed to study the behaviors and operations of a typical supply chain network under both normal and disruption conditions. By combining the characteristics of agent-based components and discrete-event models together, this hybrid simulation model enables the close observation of the internal manufacturing processes for each facility, as well as the implementation of counterfeit parts inspection/detection procedure in detail. Several performance metrics are designed to evaluate the system's resilience under the threat of counterfeit events and to compare the effectiveness of the proposed countermeasures.

2.1. Supply chain configuration

The manufacturing supply chain is modeled as a network where the nodes represent facilities such as suppliers, manufacturing plants, distribution centers (DCs), and customers, while the arcs represent relationships among these facilities and transportation links. The simulation model is developed in anyLogic [28], a Java-based simulation software supporting agent-based and discrete-event modeling applications.

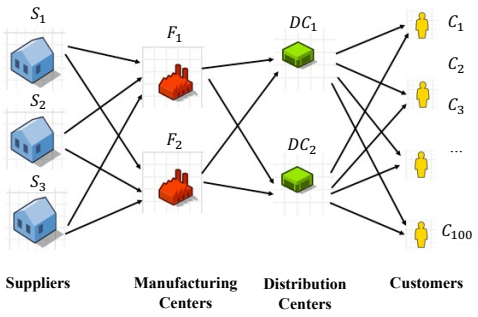


Fig. 2. Supply chain network.

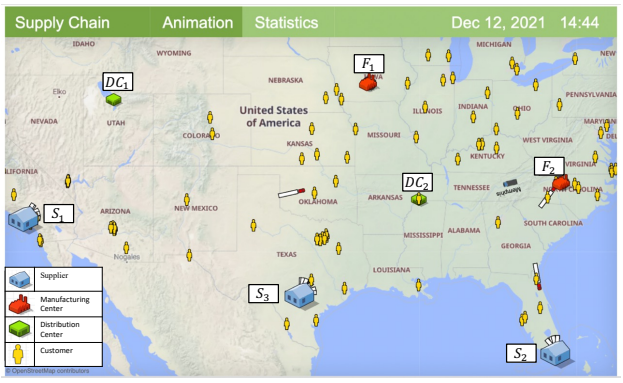


Fig. 3. Supply chain facility location map.

A simple yet realistic 4-stage manufacturing supply chain network as shown in Fig. 2 illustrates the approach. It has facility locations across the US, as shown in Fig. 3. The network consists of three suppliers (S_1, S_2, and S_3, located in Los Angeles, San Antonio, and Miami), two manufacturing centers (F_1 and F_2, located in Greensboro and Des Moines), two distributors (DC_1 and DC_2, located in Salt Lake City and Memphis), and n = 100 customers ($C_1, C_2, \ldots, C_n$, randomly located in the US).

The three suppliers together provide five different components (screen, keyboard, motherboard, battery, and laptop base) to the manufacturing centers. Manufacturing centers assemble the components into laptops. Finished laptops are delivered to DCs and then to customers. This supply chain configuration has been used in the authors' previous study [29] on the resilience of manufacturing supply chains under disruptions due to natural hazards.

Nomenclature

p_i	proportion of a manufacturing center's demand fulfilled by supplier i
d_j	proportion of a distribution center's demand fulfilled by manufacturing center j
n	number of customers in the supply chain network
p_T	proportion of counterfeit parts in parts provided by trusted suppliers
p_C	proportion of counterfeit parts in parts provided by commercial off-the-shelf (COTS) suppliers
s_1	proportion of incoming parts selected for standard inspection at manufacturing center
a_1	accuracy of standard inspection
t_1	unit inspection time for standard inspection
s_T	proportion of incoming parts provided by trusted suppliers selected for tight inspection
s_C	proportion of incoming parts provided by COTS suppliers selected for tight inspection
a_2	accuracy of tight inspection
t_T	unit inspection time for tight inspection on parts provided by trusted suppliers
t_C	unit inspection time for tight inspection on parts provided by COTS suppliers
P	total number of counterfeit parts in the system
FN	number of undetected counterfeit parts
FN_T	number of undetected counterfeit parts from trusted suppliers
FN_C	number of undetected counterfeit parts from COTS suppliers
β	proportion of undetected counterfeit parts
β_T	proportion of undetected counterfeit parts from trusted suppliers
β_C	number of undetected counterfeit parts from COTS suppliers
FN_t	number of undetected counterfeit parts on day t
P_t	total number of counterfeit parts on day t
β_t	proportion of undetected counterfeit parts on day t
Q_t	scheduled production quantity on day t
$\tilde{Q}_t$	actual production quantity on day t
t_0	unit production time for assembling a laptop

2.2. Baseline scenario

There is no counterfeit threat in the baseline scenario. All suppliers are considered trustworthy; hence they provide authentic components continuously to the manufacturing centers for assembly. Production at the manufacturing centers is not interrupted by counterfeit parts, and no additional inspection is needed. The parameters in the SC network are designed so that it can meet customers' daily demands without delay. The system maintains undisrupted operations throughout the entire simulation period.

The hybrid simulation model is developed by implementing multiple discrete event modules inside every facility agent type. The discrete event modules are embedded with the essential functionalities for the normal operations of the agent. These discrete event modules have their own triggering mechanisms and work cooperatively to form the facilities' characteristics. Multiple replicate instances of the same agent type have identical behaviors and properties but operate independently. For example, the agent of type customer has $n = 100$ instances generated at the beginning of the simulation, mimicking each customer's daily behavior.

The communication flowchart and the detailed system structure are explained in Fig. 4. The blocks represent the facility entities in the supply chain network and have the major functionalities for each facility inside. The *Transport* arrows between blocks indicate the direction that packages follow. For example, a *Transport* arrow between the *Supplier* block and the *Manufacturing center* block shows that raw materials/components are transported from the *Supplier* agent to the *Manufacturing center* agent.

Similarly, the *Demand* arrow in Fig. 4 represents the direction of the demand that a facility type passes to another. Instances of each facility will communicate with instances from their adjacent agent types in real time. The working mechanisms of the four major facilities in the supply chain network are described below.

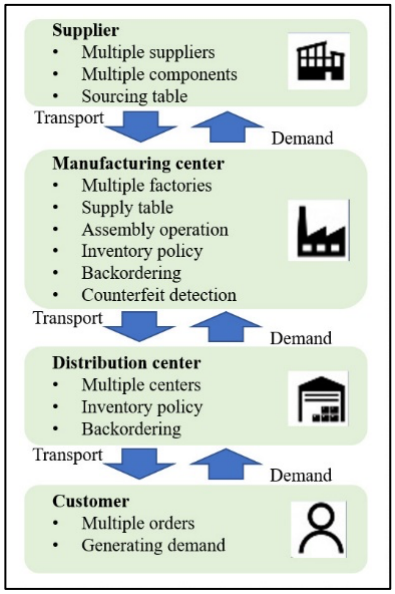


Fig. 4. Flowchart explaining the agents and communications in simulation.

Suppliers provide five components (laptop base, motherboard, battery, keyboard, and screen) to manufacturing centers to assemble into laptops. Each of the five components is shipped from a supplier to a manufacturing center according to a pre-specified ratio. Manufacturing center F_i 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 the sourcing table (Table 2). For example, both manufacturing centers receive all of their screens from S_1. F_2 receives 40% of the keyboards from S_1 and the remaining 60% from S_2. The transportation between a supplier and a manufacturing center takes 5 hours.

A supplier agent may come from one of two sources: the trusted/qualified suppliers source or the COTS suppliers source. The specific setup is discussed in the threat and countermeasure scenarios. When no counterfeit event occurs, all suppliers are considered trustworthy, and there will be no counterfeit parts in the network. Supplier agents are simplified to have unlimited raw component storage since they are not the focus of this study.

Table 2. Sourcing table showing proportions of components from each supplier to each manufacturing center.

(p_1, p_2, p_3)	F_1	F_2
Screen	(1, 0, 0)	(1, 0, 0)
Keyboard	(0.4, 0.6, 0)	(0.4, 0.6, 0)
Motherboard	(0, 0.45, 0.55)	(0, 0.45, 0.55)
Battery	(0, 0.5, 0.5)	(0, 0.5, 0.5)
Laptop base	(0, 0, 1)	(0, 0, 1)

Manufacturing centers receive demand orders from distribution centers and need to produce laptops to satisfy their demands. The five types of required components have a starting inventory of 1,000 units for each type and starting laptop inventory of 1,500 units. The QR inventory policy (fixed replenishment quantity policy) is applied separately to laptops and each type of raw component with $(Q, R) = (1000, 600)$. Each manufacturing center produces laptops at a stable throughput rate of $Q_t = 150$ units/day. Manufacturing centers will stop receiving raw components or produce new laptops when the inventory reaches 1500 for the corresponding types.

Distribution centers deliver orders of finished laptops to customers. DCs have starting inventory of 1,500 units. They also use the QR inventory policy with $(Q, R) = (1000, 600)$. The demand received by each DC will be divided into d_j (j = 1, 2) proportion and sent to the two manufacturing centers. DC_1's demand is fulfilled by F_1 and F_2 equally, $d_1 = (0.5, 0.5)$; DC_2 has $d_2 = (0.4, 0.6)$, meaning that 40% of DC_2's demand is fulfilled by F_1 and 60% by F_2. The transportation between a manufacturing center and a DC takes 5 hours.

The *Customer* agents will place daily demand with the laptop amount according to a uniform distribution of $U(1,3)$. These demand orders will be sent to the nearest DC(s). Based on the network configuration in Fig. 3, there are 45 customers located near DC_1, and the rest of the 55 customers are much closer to DC_2. The transportation between a DC and a customer takes 3 days, regardless of the specific geolocation assigned to the customers.

2.3. Counterfeit parts threat scenario

In the counterfeit parts threat scenario, counterfeit events occur, but no countermeasures are introduced. We assume only motherboards are affected by counterfeits, while the other four types of components are unaffected. When a counterfeit event occurs, suppliers that provide motherboards have a certain proportion of counterfeit parts flowing into manufacturing centers. Laptops assembled with counterfeit motherboards are considered defective products. During a counterfeit event, which has an occurrence frequency of at least once a year, trusted/qualified suppliers have p_T (%) counterfeit motherboard units mixed into their reorder amount, while COTS suppliers contain p_C (%) of counterfeit units. These percentages are determined by the probability distributions of event severities, based on historical data from suppliers. Table 3 provides the specified counterfeit event parameters. The severity of the counterfeit event is classified into three levels: low, medium, and high.

As shown in Table 3, the low severity events represent 50% of all counterfeit events; 5% of the motherboards provided by trusted/qualified suppliers are counterfeit, and 20% of the motherboards provided by COTS suppliers are counterfeit. The medium severity events represent 30% of all counterfeit events, with higher p_T and p_C values than the low severity event. The high-severity events represent 20% of all counterfeit events, with the highest p_T and p_C values compared to the medium- or low-severity events.

Table 3. Counterfeit event parameters in the threat scenario.

Severity	Probability	p_T (%)	p_C (%)
Low	0.5	5	20
Medium	0.3	10	25
High	0.2	15	30

2.4. Countermeasure scenarios

Three different CMs (CM1, CM2, and CM3) have been developed to provide resilience during disruptive events caused by counterfeits.

2.4.1. CM1: Database search

One of the first actions in identifying potential threats due to counterfeit parts is database searching. There are two well-known databases for counterfeits: the Government-Industry Data Exchange Program (GIDEP) by DoD and the ERAI High Risk and Suspect Counterfeit Parts Database by ERAI Inc. GIDEP [30] is a cooperative activity between government and industry participants seeking to reduce expenditures of resources by sharing technical information about counterfeit products. Likewise, Electronic Resellers Association International (ERAI) was founded in 1985 as a major resource for checking if a component is counterfeit [31]. It is the world's largest database of suspect counterfeit and nonconforming electronic parts. These two sources in addition to the DoD Trusted Suppliers list constitute the first "line of defense" to check for counterfeits parts.

CM1 applies a standard sampling inspection module on the assembly lines for incoming motherboard units in the manufacturing centers, as shown in Fig. 5. This inspection module represents the time needed for searching the GIDEP and ERAI databases to check if an incoming motherboard unit is listed as counterfeit or not. Specifically, we assume $s_1 = 20\%$ of incoming motherboard units will be sent to the inspection module for examination, and the examination has an accuracy of $a_1 = 90\%$. The unit inspection time t_1 (minutes) follows triangular distribution $\mathrm{tri}(10, 20, 15)$.

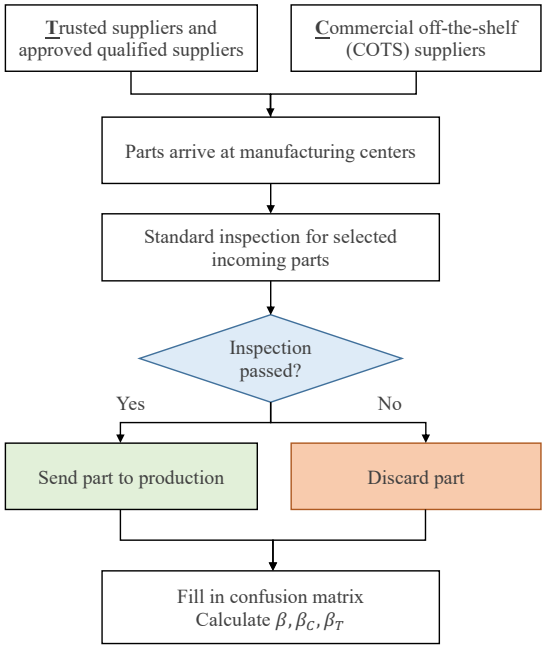


Fig. 5. Flowchart for the manufacturing center agent in CM1.

Confusion Matrix		Inspection outcome: Good	Inspection outcome: Counterfeit		
Ground truth	C-Good	TN_C	FP_C	N_C	N
	T-Good	TN_T	FP_T	N_T	
	C-Counterfeit	FN_C	TP_C	P_C	P
	T-Counterfeit	FN_T	TP_T	P_T	

Fig. 6. Format of the confusion matrix for manufacturing centers.

Parts detected as counterfeits will be discarded, while those that have passed the inspection will be sent to the assembly line for production, along with the unselected parts. Statistics are continuously tracked and recorded in the form of a confusion matrix, as shown in Fig. 6.

2.4.2. CM2: Increased inspection and detection

(a) The countermeasure procedure

CM2 policy implements a tight inspection mechanism in addition to the standard database search in CM1, as shown by the flows inside the red box in Fig. 7. Once parts arrive at the manufacturing centers, they are passed through different inspection modules, depending on the threshold mechanism, which will be elaborated in the next section. If tight inspection is not triggered, we simply follow the right branch, which is the standard inspection module CM1. Standard inspection is applied to $s_1 = 20\%$ of selected incoming motherboards with accuracy $a_1 = 90\%$.

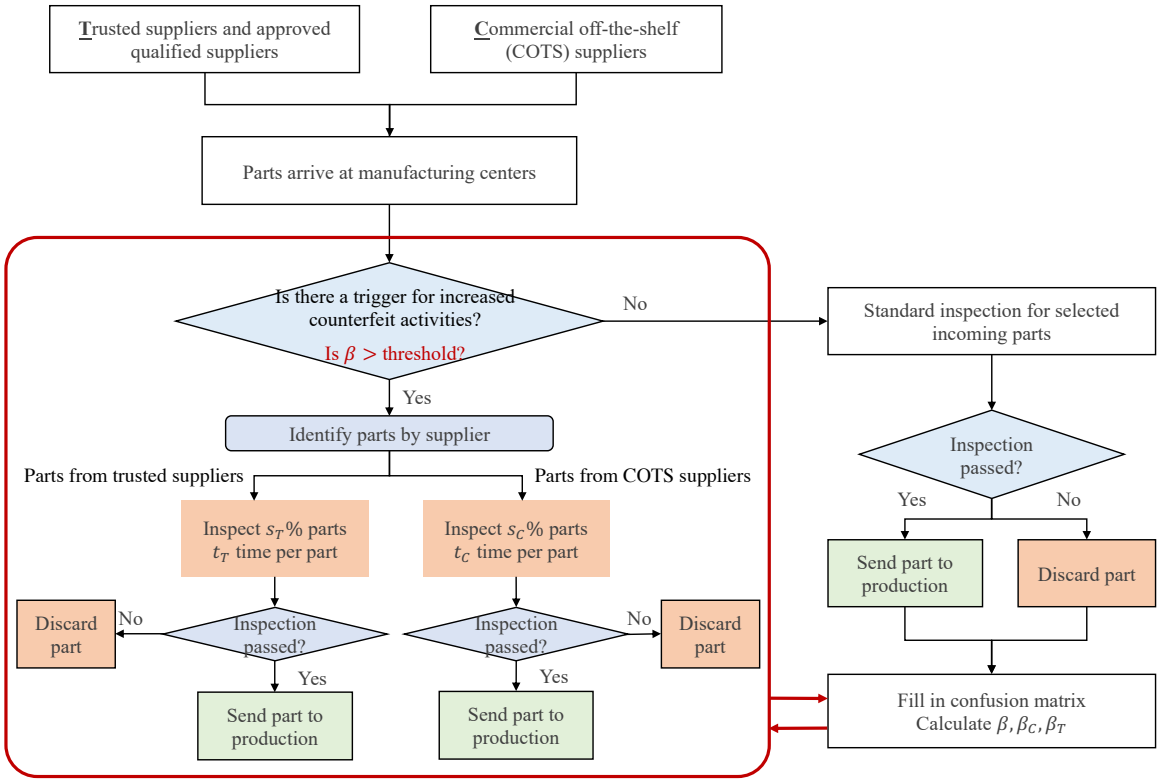


Fig. 7. Flowchart for the Manufacturing center agent in CM2.

If tight inspection is triggered, we continue into the red box flow in Fig. 7. Parts from trusted suppliers and COTS suppliers will be sent to separate inspection lines. Because we have more confidence in the trusted suppliers, we select s_T = 40% of the motherboards from trusted suppliers for the tight inspection, while s_C = 50% of the motherboards from COTS suppliers will be selected. We assume the accuracy of tight inspection is $a_2 = 95\%$, and the unit inspection times t_T for trusted suppliers and t_C for COTS suppliers both follow triangular distribution $\mathrm{tri}(15, 25, 20)$. The tight inspection takes more time than standard inspection but has higher accuracy. Parts detected as counterfeits will be discarded, while those pass the inspection will be sent to the assembly line for production, along with the unselected parts.

(b) The triggering mechanism

As shown by the triggering condition in Fig. 7, the tight inspection is triggered when the threshold is met due to increased counterfeit activities. The threshold mechanism is controlled by the β value, which can be defined as:

$$FN = FN_C + FN_T \tag{1}$$

$$\beta = \frac{FN}{P} \tag{2}$$

using the notations given in Fig. 6. The β value is a dynamic value that reflects the proportion of undetected counterfeit parts in the system. In this simulation, both the accumulative amount β and the daily incremental amount β_t are recorded:

$$\beta_t = \frac{FN_t}{P_t} \tag{3}$$

When there's no counterfeit event in the SC, β and β_t should remain at the default zero. For the kth counterfeit event, suppliers start to send counterfeit parts to manufacturing centers at day t_k, but this won't have an immediate impact on the final products until manufacturing centers use up all the previous inventory. After a delay d, on day t_{k+d}, production starts to use the received components containing counterfeit parts, and this is when the counterfeit event starts to get noticed. Therefore, the daily β_t starts to become positive as counterfeit parts are passed through the assembly line. The β value will also rise from zero as counterfeit parts continuously are flowed into production.

A proposition can be drawn that when $\beta_t > 0$, there must be bad parts that have gone through the system on that day. β_t will maintain 0 when there are no counterfeit parts detected as authentic parts on that day. Furthermore, β is unchanged if no counterfeit part is recorded. Although with the tight inspection accuracy a_2 and selecting rates in the tight inspection lines, and the stochastic distribution of good and bad parts in the inventory, there is still a chance that bad parts remain in the inventory when $\beta_t = 0$ for this day and a fixed threshold mechanism will be easily triggered to turn off the tight inspection module. However, it cannot be guaranteed whether there still be remaining bad parts in the inventory until the β_t maintains zero for an extended period; hence the tight inspection module should not be turned off under such circumstances. A more reasonable way to define

the threshold is to monitor β_t for a consecutive number of days, and then evaluate the conditions continuously.

In this study, we design CM2 to have β_t values recorded for five consecutive days based on the experimental results with a fixed threshold, as five days is believed to be sufficient to eliminate the possibility of remaining bad parts in the inventory. If β_t value is maintained at zero for the given time window, then we are confident that the counterfeit event ends. The EWMA method is applied to monitor the dynamic threshold to decide when to turn off the tight inspection module. EWMA [32] utilizes the exponential weighted moving average of the target values in the given time window. A counterfeit event is identified when the EWMA value is changed from zero to a positive value, indicating that in the past five days, β_t value is increased from zero, so the tight inspection module should be turned on. When EWMA is reduced to zero, indicating that no more counterfeit parts are detected for the past 5 days, then the tight inspection module can be turned off.

With this triggering mechanism developed, the activity of counterfeit events can be appropriately measured, and the tight inspection module can be turned on and off promptly. This triggering mechanism can be further extended to include the daily β_T and β_C for the proportion of undetected counterfeit parts from trusted suppliers and COTS suppliers, respectively, in addition to the overall β. By comparing β_T and β_C to their respective thresholds, we can turn on/off the tight inspection for only one branch (only for trusted suppliers or only for COTS suppliers) or both branches, allocating the counterfeit inspection and detection resources more strategically.

(c) The stopping mechanism

When the inspection modules inside manufacturing centers can correctly distinguish counterfeit parts from the rest of the incoming parts, suppliers will have no incentive of sending counterfeit parts. This signals the end of the counterfeit event. We monitor the EWMA values for three consecutive up-and-down periods. If the EWMA values drop below a threshold, it indicates that manufacturing centers can handle counterfeits effectively, and so it will be reasonable for manufacturing centers to send a stopping signal to suppliers; suppliers then stop sending counterfeit parts.

2.4.3. CM3: CM2 with dynamic production capacity

CM3 is an improvement of CM2 to address the lost production time due to tight inspection. We implement a discrete event module for manufacturing centers to control the daily scheduled production quantity Q_t . In our simulation, the actual daily production amount $\tilde{Q}_t$ is recorded. In the baseline scenario, $\tilde{Q}_t = Q_t$ since there is no counterfeit threat in the baseline.

When countermeasures are implemented, some production time will be lost due to the time in inspection, especially the tight inspection in CM2 that takes longer and inspects more parts, resulting in $\tilde{Q}_t < Q_t$. This will cause delayed or unfulfilled orders to DCs and customers. Therefore, the production control module in CM3 will increase $\tilde{Q}_{t+1}$ when seeing $\tilde{Q}_t < Q_t$, forcing the manufacturing centers to speed up production the next day. With the dynamic control of daily scheduled production, manufacturing centers can maintain throughput at a high level to compensate for the time spent on the inspection.

Table 4 summarizes all five scenarios and their parameters.

Table 4. Scenario description and parameters.

Model	Description
Baseline	• Normal operation without disruptions
Threat only (counterfeit motherboards from suppliers)	• Counterfeit events occur but no CMs are applied • Start of the threat event: random, at least one event in a year • Three levels of threat severity • End of the threat event: when β drops below a threshold for a period, indicating that counterfeit activities are detected at the manufacturing centers, and so suppliers will have no incentive of sending counterfeit parts
Threat + CM1 (database search)	• Select 20% of all incoming parts and compare them to databases (GIDEP and ERAI) • Inspection time ~ tri(10,20,15), accuracy = 90%
Threat + CM2 (increased inspection and detection)	• Database search included • Trigger increased inspection and detection when $\beta > 0.1$ • Inspect 60% of parts from COTS suppliers and 50% of parts from trusted suppliers • Inspection time ~ tri(15,25,20), accuracy = 95%
Threat + CM3 (increased inspection and detection with dynamic production capacity)	• Database search included • Increased inspection and detection included • Manufacturing centers adjust production plan every day: increase production capacity to compensate for the time lost in increased inspection and detection

2.5. Performance metrics

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

(1) Good Product Proportion shows the accumulative good product proportion of a given facility based on the number of laptops received that do not contain counterfeit parts to the total number of laptops received:

$$GPP^{(i)} = \frac{GPL}{TL} \tag{4}$$

where i is the facility index, GPL is the number of good products received, and TL is the total number of products received.

(2) Service Level by Products shows the service level based on the ratio of the total number of products in the successfully fulfilled orders to the sum of products in all orders placed for the facility:

$$SLP^{(i)} = \frac{PSO}{PSO + PUO} \tag{5}$$

where PSO is the number of products in the successfully fulfilled orders, and PUO is the number of products in the unsuccessful fulfilled orders.

(3) ELT Service Level by Products is the service level based on the ratio of the total number of products in on-time orders to the overall number of products in outgoing orders:

$$ELTSLP^{(i)} = \frac{POTO}{POTO + PDO} \tag{6}$$

where $POTO$ is the number of products in on-time orders, and PDO is the number of products in delayed orders.

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

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

3. Results

For each scenario, 30 replications are performed with a one-year duration to capture enough counterfeit and recovery situations. The experimental results are collected for CMs with the fixed parameter (FP) experiment. Parameters for CMs models are fixed to the default values introduced in the scenario section to simulate the supply chain under relatively deterministic conditions. The performance metrics are collected in each distribution center to reflect the regional impacts of the counterfeit event on customers.

3.1. Results comparing the three countermeasures

Since DCs are direct downstream from manufacturing centers, the DCs' performance directly reflects how manufacturing centers are meeting demands. Focusing on the performance metrics for each DC, we summarize their simulation results in Table 5. We use 30 replications of each scenario, for the Central Limit Theorem to hold. The cells display the average and standard deviation values (in the brackets) of the 30 replications across each performance metric and each scenario.

We can observe that CM1 outperforms others on the *service level*, *ELT service level*, and *average delivery time* performance metrics, while CM2 scores the worst across all scenarios. CM3 can maintain high performance in the *service level*, *ELT service level*, and *average delivery time* metrics for all DC_1 results. DC_2 results are also close to the desired values. CM2 results in the highest *GPP* values of 0.9853 for DC_1 and 0.9858 for DC_2, while CM1 performs the worst, at 0.9568 for DC_1 and 0.956 for DC_2. CM3 has comparable values with CM2.

The *performance effectiveness* (PE) column in Table 5 calculates the performance effectiveness compared to the *threat only* scenario. PE quantifies the harm reduced by the countermeasure. For example, CM3 reduces the harm of counterfeit events in DC_1 from (1-0.9506) to (1-0.9846), by 68.826%. CM2 and CM3 are the scenarios having an average of around 70% effectiveness to the threats, while CM1 only has around 12% effectiveness in the face of resisting the threats.

To further explain the *GPP* metric, boxplots of the *GPP* metric from all replications are presented in Fig. 8(a). The *GPP* metric directly reflects the effectiveness of countermeasure policies, while other metrics are more related to the supply chain network's ability to satisfy the demands during the affected period. All CMs help to reduce the impact to some extent when compared to the *threat only* scenario, while CM2 and CM3 are comparable in this metric. CM1's performance is slightly better than the *threat only* scenario because using the standard inspection module alone is not sufficient to mitigate the impact of the counterfeit events. The high variance value of CM1 indicates that across the 30 replications, the performance of CM1 is not stable, highly depending on the counterfeit event severity, and the ability of CM1 to resist the counterfeit disruptions is lower than those of CM2 and CM3. Fig. 8(b) provides a close look at the *GPP* value change of DC_1 for a single replication of each scenario throughout the simulation period. The plot for DC_2 is similar to that of DC_1. The significant drop in performance level at the beginning of the plot reflects the start of the counterfeit event. Similar situations can be observed for both distribution centers. However, CM2 and

Table 5. Performance of each distribution center for each simulation scenario, showing the average and standard deviation from 30 replications.

Scenario	Service level by products (SLP)		ELT Service level by products (ELTSLP)		Average delivery time		Good product proportion (GPP)			
	DC1	DC2	DC1	DC2	DC1	DC2	DC1	PE (%)	DC2	PE (%)
Threat only	1.000 (0.000)	1.000 (0.000)	1.000 (0.000)	1.000 (0.000)	3.000 (0.000)	3.000 (0.000)	0.951 (0.045)	-	0.950 (0.044)	-
Threat + CM1	1.000 (0.000)	1.000 (0.000)	1.000 (0.000)	1.000 (0.000)	3.000 (0.000)	3.000 (0.000)	0.957 (0.039)	12.55	0.956 (0.039)	11.29
Threat + CM2	0.989 (0.053)	0.980 (0.077)	0.991 (0.045)	0.984 (0.066)	3.2 00 (1.095)	3.700 (2.806)	0.985 (0.023)	70.24	0.986 (0.022)	71.37
Threat + CM3	1.000 (0.000)	0.998 (0.008)	1.000 (0.000)	0.999 (0.003)	3.000 (0.000)	3.000 (0.000)	0.985 (0.022)	68.83	0.985 (0.022)	69.76

CM3 can quickly bounce back from the disruptions after the performance drops to around 0.95. At the same time, the *threat only* and CM1 scenarios are not able to recover, as the counterfeit event never ends in these two scenarios.

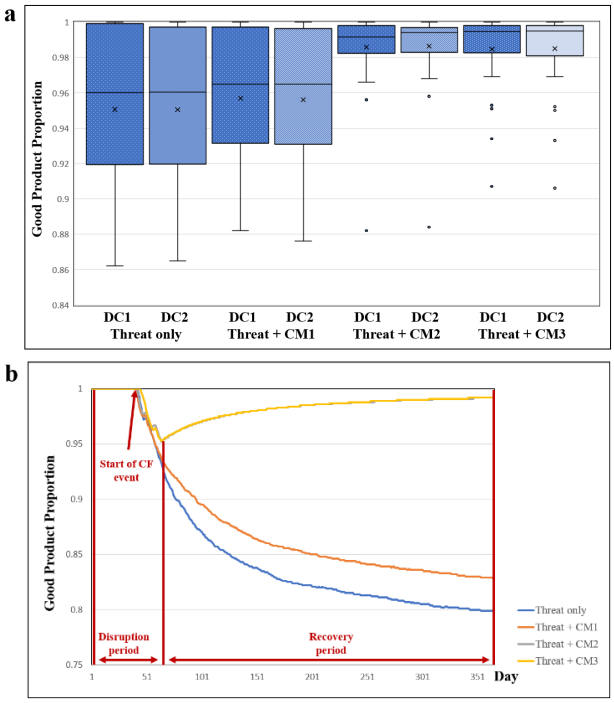


Fig. 8. Simulation results: (a) Boxplots of GPP for 30 replications; (b) GPP of DC_1 from a single run.

3.2. Discussion

Based on the simulation results from all scenarios, it can be seen that all three countermeasures improve the *GPP*. However, CM1 is the least effective countermeasure because only a standard inspection module is adopted in this scenario. The module's accuracy is not as effective as those in CM2 and CM3.

The standard inspection time will not delay the system significantly in the FP experiment; hence CM1 can stay at perfect performance on the *service level*, *ELT service level*, and *average delivery time* performance metrics. The low values of CM2 are due to the longer inspection time during tight inspection. Without the dynamic production control mechanism in CM3, CM2 cannot maintain the requested daily production. Therefore, these performance metrics for CM2 are affected significantly. CM3's performance on these three metrics is barely affected; they are mainly at the perfect values.

Since a customer's daily ordering amount follows a uniform distribution $U(1,3)$, the expected daily laptop demand from all 100 customers is $100 \times E(X_t \sim U(1,3)) = 200$. There are two DCs, with 45% and 55% split demand ratio, DC_1 has an average of $200 \times 45\% = 90$ demands per day, and DC_2 has an average of $200 \times 55\% = 110$ demands per day. The two manufacturing centers have a 1:1 supply ratio of receiving orders from each distribution center. For a given pair of parameter combination, manufacturing centers may take more time on inspection due to the increase of selecting-rate-related parameters s_1, s_T, s_C, and the decrease in accuracy-related values a_1, a_2, which ends up lowering the actual daily production $\tilde{Q}_t$ consequently. Hence, the service level is below 1 when the total daily production of both manufacturing centers is less than the demand from distribution centers.

For CM1, the counterfeit event has an extended affected period than CM2 when no stopping mechanism is implemented to stop the counterfeit event; hence the *service level* of CM1 reaches a lower but relatively more stable level after accumulation. For CM2, the affected period is shorter than CM1, but the lingering effects from the counterfeit threat period can continuously impact the system because the production loss recovers very slowly. For CM3, the dynamic production control mechanism adjusts the daily production; hence faster production-loss-recovery is enabled. There will still be products stored in inventory in addition to satisfying the daily demands. The surplus production can clear up the backlog orders faster, thus reducing the *service level* loss.

4. Conclusion

As a result of the persistence and aggravation of the counterfeit market pausing a real threat to people's safety and economy, the need to implement effective counterfeit countermeasures grows. Furthermore, assessing the countermeasures to be implemented based on the system's performance metrics makes a perfect decision-making tool. This paper presented a model for implementing different countermeasures for counterfeited motherboards in an ICT manufacturing supply chain and studied the system's resilience after the disruptions. The probability distribution for the model parameters was found based on elicitation to find the actual effectiveness of each scenario and obtain more practical results. However, the network model is easy to reconfigure and used for other supply chain networks. The model assessed the system's performance in three different scenarios and showed the effectiveness of implementing the beta trigger policy with a dynamic production scenario (CM3).

The work done in this paper opens opportunities for further studies to combat counterfeiting. One crucial direction would be considering the events of having counterfeits in more than one type of component with different probabilities of occurrence and criticality. Here, further investigations considering the cost-benefit analysis of increasing the tightness of the inspection measures in wider-range problems will be of great importance. Future research can also examine the combination of other threats disrupting the supply chain and the counterfeits threat. Other threats can be due to environmental disasters, political incidents, or supply disruptions.

Acknowledgements

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.

References

[1] Business Week, "The Counterfeit Trade: Illegal Copies Threaten Most Industries and Can Endanger Consumers", in *Business Week*. 1985. pp. 64-72.

[2] SAE International, "SAE AS5553 Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition Standards". 2019, SAE International.

[3] Department of Defense, "DoD Instruction 4140.67, "DoD Counterfeit Prevention Policy," ". 2013, DOD.

[4] Department of Defense, "Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012–D055) ". 2014.

[5] Frontier Economics Ltd, "THE ECONOMIC COSTS OF COUNTERFEITING AND PIRACY". 2017.

[6] OECD and European Union Intellectual Property Office, *Trends in Trade in Counterfeit and Pirated Goods*. Paris Illicit Trade, OECD Publishing, 2019.

[7] U. Guin, D. DiMase, and M. Tehranipoor, "A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment," *Springer Science*, 2013.

[8] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoorand, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *IEEE*, 2014.

[9] U.S. Department of Commerce Bureau OF Industry and Security Office of Technology Evaluation, "DEFENSE INDUSTRIAL BASE ASSESSMENT: COUNTERFEIT ELECTRONICS". 2010.

[10] The European Observatory on Infringements of Intellectual Property Rights, "ANTI-COUNTERFEITING TECHNOLOGY GUIDE". 2021, European Union Intellectual Property Office.

[11] S. K. Kwok, J. Ting, A. Tsang, W. B. Lee, and B. Cheung, "Design and development of a mobile EPC-RFID-based self-validation system (MESS) for product authentication," *Elsevier*, 2010.

[12] S. L. Ting and A. Tsang, "A two-factor authentication system using Radio Frequency Identification and watermarking technology," *Elsevier*, 2012.

[13] K. Hendricks and V. Singhal, "An Empirical Analysis of the Effect of Supply Chain Disruptions on Long‐Run Stock Price Performance and Equity Risk of the Firm," *Production and Operations Management*, vol. 14, pp. 35-52, 2005.

[14] S. Ponis and E. Koronis, "Supply Chain Resilience: Definition Of Concept And Its Formative Elements," *Journal of Applied Business Research*, vol. 28, pp. 921-929, 2012.

[15] U. Soni, V. Jain, and S. Kumar, "Measuring supply chain resilience using a deterministic modeling approach," *Comput. Ind. Eng.*, vol. 74, pp. 11–25, 2014.

[16] V. Jain, S. Kumar, U. Soni, and C. Chandra, "Supply chain resilience: model development and empirical analysis," *International Journal of Production Research*, vol. 55, no. 22, pp. 6779-6800, 2017.

[17] A. Oke and M. Gopalakrishnan, "Managing disruptions in supply chains: A case study of a retail supply chain," *Elsevier*, 2008.

[18] L. V. Snyder, Z. Atan, P. Peng, Y. Rong, A. J. Schmitt, and B. Sinsoysal, "OR/MS models for supply chain disruptions: A review," *IIE Transactions (Institute of Industrial Engineers)*, vol. 48, no. 2, pp. 89-109, 2016.

[19] L. V. Snyder, M. P. Scaparra, M. S. Daskin, and R. L. Church, "Planning for Disruptions in Supply Chain Networks," *INFORMS TutORials in Operations Research*, 2014.

[20] D. A. Ghadge, A. Duck, M. Er, and N. Caldwell, "Deceptive counterfeit risk in global supply chains," *Supply Chain Forum: An International Journal*, vol. 22, pp. 1-13, 2021.

[21] I. Miyamoto, T. H. Holzer, and S. Sarkani, "Why a counterfeit risk avoidance strategy fails," *Elsevier*, 2017.

[22] D. DiMase, Z. A. Collier, J. Carlson, R. B. Gray Jr., and I. Linkov, "Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains for Complex Systems," *Risk Analysis*, vol. 36, no. 10, pp. 1834-1843, 2016.

[23] N. Etemadi, Y. Borbon-Galvez, F. Strozzi, and T. Etemadi, "Supply Chain Disruption Risk Management with Blockchain: A Dynamic Literature Review," *Information*, vol. 12, no. 2, p. 70, 2021.

[24] V. Mani, J. M. Swaminathan, and A. Alpteknoglu, "Counterfeit Risk : Supply Chain Drivers and Mitigation Strategies". 2018: Kenan‐Flagler Business School, University of North Carolina.

[25] E. Gossena, J. Eckardta, and E. Abele, "Anti-counterfeiting effectivity analysis using attack and defense tree scenario methods," *Elsevier*, 2015.

[26] D. A. Bodner, "Enterprise Modeling Framework for Counterfeit Parts in Defense Systems," *Procedia Computer Science*, vol. 36, pp. 425-431, 2014.

[27] D. A. Bodner, "Mitigating Counterfeit Part Intrusions with Enterprise Simulation," *Procedia Computer Science*, vol. 61, pp. 233-239, 2015.

[28] A. B. I. Grigoryev, *The Big Book of Simulation Modeling*. https://www.anylogic.com/resources/books/big-book-of-simulation-modeling/ anylogic company, 2013.

[29] W. G. Guo, P. Kantor, E. Elsayed, E. Rosenberg, R. Lei, S. Patel, B. Ruskey, and F. Roberts, "Supply Chain Threats and Countermeasures: From Elicitation through Optimization," *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2022.

[30] GIDEP, https://www.gidep.org/about/about.htm.

[31] ERAI, https://www.erai.com/aboutus_profile.

[32] S. W. Roberts, "Control Chart Tests Based on Geometric Moving Averages," *Technometrics*, vol. 1, no. 3, pp. 239-250, 1959.