Strategic Discourse Quarterly
Vol II. No V. Summer 2025
Pages 107-131

Simulation of Defense Supply Chain Resilience Strategies Using Wargaming Scenarios: Analysis and Evaluation

Morteza Pourjafari[1], Mohammad Saeed Alamdari[2], Reza Etesami[3]

Receipt Date: 2025/06/13 Date of Acceptance: 2025/07/18

Abstract

The resilience of the defense supply chain, as one of the key factors in safeguarding national security and sustaining the operational capability of armed forces, is of paramount importance. Given the wide range of threats faced by defense supply chains, this study examines and evaluates the resilience of the defense supply chain through simulation and wargaming scenarios. In this research, the R software and the Simmer simulation tool were employed to model the defense supply chain, encompassing suppliers, manufacturers, warehouses, and transportation. Various scenarios—including cyberattacks, logistics delays, equipment failures, physical threats, natural crises, economic sanctions, and sudden changes in demand—were defined and simulated in order to assess the resilience of the chain. The simulation results indicate that economic sanctions exert the most significant impact on the resilience of the defense supply chain and can seriously disrupt the procurement of raw materials and critical components. Equipment failures and logistics delays were also identified as major threats that could reduce efficiency and cause disruptions in supply chain processes. Other threats, such as cyberattacks and physical threats, were found to be significant due to their indirect effects on the infrastructure and operations of the supply chain. This study demonstrates that through the adoption of targeted strategies—such as diversification of supply sources, optimization of transportation routes, strengthening of cybersecurity infrastructure, and preventive equipment maintenance—the resilience of the defense supply chain can be considerably enhanced, thereby mitigating the destructive consequences of critical threats. The findings can assist decision-makers in adopting effective policies and strategies aimed at improving the resilience of defense supply chains.

Keywords: Defense Supply Chain, Resilience, Wargaming, Simulation, Logistics Processes.

[1] Ph.D. in Strategic Defense Sciences – Research Institute of Logistics, Defense Technology and Emerging Fields – Supreme National Defense University – Tehran, Iran
[2] Ph.D. in Mathematics – Research Institute of Logistics, Defense Technology and Emerging Fields – Supreme National Defense University – Tehran, Iran
[3] Ph.D. Candidate – Faculty of Mathematics and Computer Science – Shahid Baher University of Ahvaz – Kerman, Iran

Introduction

The defense supply chain, as the backbone of military operations and national security, plays a vital role in providing equipment, logistics, and resources required by the armed forces. With the increasing complexity and diversity of threats, the resilience of these supply chains has become a fundamental challenge for governments and military organizations. Supply chain resilience refers to its ability to withstand unexpected events and to return to its original state, or even improve, after a crisis. This resilience is essential not only for maintaining operational efficiency but also for safeguarding national security (Lucas et al., 2024).

Rapid technological developments, the intensification of cyber threats, geopolitical changes, and economic sanctions are only some of the challenges confronting defense supply chains. Any disruption in these chains may result in reduced military capability and the emergence of serious vulnerabilities. Therefore, analyzing and strengthening the resilience of the defense supply chain is regarded as a top priority in strategic defense planning and management (Ormiston et al., 2024). Simulation methods and wargaming scenario analyses are powerful tools for evaluating and enhancing supply chain resilience. These approaches, by creating simulated environments, provide the opportunity to examine the reactions of the supply chain to various threats and crises (Mostafa et al., 2021). In this regard, the use of advanced simulation software such as **Simmer** in the renvironment can contribute to more precise and comprehensive analysis.

This research seeks to simulate and evaluate strategies for enhancing the resilience of the defense supply chain using wargaming scenarios. In this simulation, various supply chain resources, including suppliers, manufacturers, warehouses, and transportation, are modeled, and key processes such as raw material acquisition, production, and delivery to customers are simulated. In addition, scenarios such as cyber-attacks, logistics delays, and equipment failures are defined in order to assess their effects on the performance and resilience of the supply chain. This study also explores methods for improving resilience through enhancing cybersecurity, improving logistics processes, and better equipment management. It is hoped that the findings of this research will assist policymakers, decision-makers, and military managers in identifying strengths and weaknesses of the defense supply chain and in adopting effective strategies to enhance its resilience. In the subsequent sections, the

article discusses simulation methods and models in greater detail, analyzes the results, and presents recommendations for strengthening defense supply chain resilience.

Theoretical Foundations

This section examines the concepts and theories related to the resilience of the defense supply chain and the application of wargaming scenarios to enhance it. The theoretical foundations of this research include the concepts of resilience, supply chain, defense supply chain, and the use of wargaming for simulation and threat analysis.

Resilience

Resilience refers to the ability of a system to return to its original state or to adapt to new conditions after encountering shocks and threats. Initially introduced in environmental sciences and psychology, the concept later expanded into fields such as engineering, management, and organizational studies. In the context of supply chains, resilience refers to the ability of the supply chain to maintain efficiency and effectiveness after disruptions and crises. Supply chain resilience includes four main components:

- **Absorptive capacity**: the ability of the supply chain to absorb shocks and disruptions without interrupting normal operations.
- **Adaptive capacity**: the ability of the supply chain to adjust and adapt to new conditions after a crisis.
- **Recovery capacity**: the speed and efficiency of the supply chain in returning to normal operations after a crisis.
- **Learning capacity**: the ability of the supply chain to learn from past experiences and improve future performance accordingly (Ponomarov & Holcomb, 2009).

Supply Chain

A supply chain is a network of organizations, individuals, activities, information, and resources involved in the production and delivery of goods and services from suppliers to end consumers. Supply chain management refers to the coordination and administration of this network to improve efficiency and reduce costs. A supply chain consists of three main components:

- **Suppliers**: providers of raw materials and components.
- **Manufacturers**: organizations and firms that transform raw materials into final products.
- **Distributors and consumers**: intermediaries and end-users who receive the products (Chopra & Meindl, 2016).

Defense Supply Chain

The defense supply chain refers to the network of suppliers, manufacturers, distributors, and consumers involved in meeting a country's military and defense needs. This chain includes the provision of raw materials, spare parts, military equipment, and services associated with defense operations. The defense supply chain faces unique challenges such as the need for high security, compliance with military standards, and rapid response to crisis situations. Key characteristics of the defense supply chain include:

- **High sensitivity to security threats**: The defense supply chain must be resistant to threats such as cyber-attacks, industrial espionage, and sabotage.
- **Need for adaptability to wartime conditions**: The defense supply chain must rapidly adjust to wartime or military crisis conditions.
- **Provision of resources in emergencies**: The defense supply chain must have the capacity to supply resources and equipment to military forces under emergency conditions (Ekström et al., 2020).

Indicators of a Resilient Supply Chain in Iran's Defense Industries

Indicators of resilience, derived from previous studies and analyses in the literature on defense supply chains, national security, and military logistics, include absorptive, adaptive, recovery, and learning capacities. These concepts highlight the ability of the supply chain to maintain functionality after disruptions and crises. Key indicators include supplier diversification, strategic reserves, cybersecurity, domestic capability, and risk management (Rahimi et al., 2018).

Considering the structural differences and specific needs of Iran's defense industry, localization of resilience indicators based on current challenges and available capacities is essential. In this research, wargaming scenarios and simulations have been designed according to the specific requirements of the country's defense industry. These scenarios, including cyber-attacks, logistics delays, and equipment failures, simulate

the most likely and realistic threats to Iran's defense supply chain. Given that the country's defense systems face diverse threats such as sanctions, cyber-attacks, and infrastructural limitations, the proposed solutions—such as strengthening cybersecurity, increasing strategic reserves, and enhancing domestic capabilities—have been tailored to national requirements.

Wargaming

Wargaming is a decision-making method that employs mathematical models, simulation, and structured scenarios based on predefined or random rules, data, and processes. It is derived from real-world situations and commander-driven battle concepts to provide an operational environment for training, strategic planning, and tactical experimentation. Wargaming serves as a testbed for evaluating strategic, operational, and tactical plans. As a futures research technique, it enables military commanders to understand adversaries, explore possible courses of action, assess outcomes, and anticipate surprises. Wargaming is an effective approach for forecasting and identifying potential future threats, thus preparing commanders for facing them. Essentially, wargaming creates a constructed environment in which safe experimentation can occur to reveal which decisions may lead to failure or success, and even to estimate the costs of actions. It is a structured process of competitive challenges presented within a simulated format (Debus, 2020).

The Role of Wargaming in Simulating Supply Chain Threats

- **Crisis scenario simulation**: Wargaming facilitates the simulation of different crisis and disruption scenarios in the supply chain, including cyber-attacks, logistics delays, equipment failures, and other threats.
- **Strategy analysis and evaluation**: Through wargaming, various strategies for addressing threats and crises can be analyzed and evaluated. These strategies include security measures, logistics process improvements, and better equipment management.
- **Training and exercises**: Wargaming serves as an educational and training tool for managers and personnel of the defense supply chain. It helps them make more effective decisions when confronted with crisis situations (Zhao et al., 2021).

Critical Wargaming Scenarios Examined in the Study

This section introduces and explains the scenarios used in the study to evaluate the resilience of the defense supply chain. The main purpose is to assess the capability of the defense supply chain in facing various threats that may impact national security and military operations. The scenarios include cyber-attacks, logistics delays, equipment failures, physical threats, natural disasters, economic sanctions, and sudden demand changes. Each scenario is elaborated upon with a focus on defense supply chain resilience:

Cyber-Attack Scenario

Cyber-attacks represent a serious threat to the defense supply chain since its communication and information systems often contain sensitive military data. In this scenario, cyber-attacks may disrupt coordination among supply chain segments, halt critical operations, or even compromise classified information. Resilience in this context depends on the strength of security protocols, backup programs, and readiness to respond swiftly to such threats (Adenka et al., 2024).

Logistics Delay Scenario

The defense supply chain is highly dependent on logistics accuracy and coordination. In this scenario, logistics problems such as poor coordination between transportation units or shortages of resources may delay the delivery of critical supplies and equipment to military forces. Resilience here involves contingency transportation planning and the use of modern technologies to enhance logistics efficiency and prevent the negative impacts of delays on defense operations (Coyle et al., 2021).

Equipment Failure Scenario

Equipment failures can disrupt the production and transportation of military equipment within the defense supply chain. This scenario simulates failures of machinery or key tools in weapons manufacturing plants or storage facilities. Resilience requires preventive maintenance programs, technical staff training, and condition-monitoring systems to detect and resolve malfunctions before they escalate into major disruptions (Coyle et al., 2021).

Physical Threat Scenario

Physical threats, such as terrorist attacks or sabotage, can target critical facilities in the defense supply chain, including warehouses and military

production centers. In this scenario, resilience encompasses physical security of facilities, construction of resistant infrastructure, and emergency plans for countering such threats (Sani et al., 2022).

Natural Disaster Scenario

Natural disasters such as earthquakes, floods, or storms can have devastating effects on the defense supply chain. This scenario investigates their impact on production shutdowns, transport delays, and storage disruptions. Resilience requires disaster-resistant infrastructure and rapid recovery systems to ensure continuity of operations with minimal interruption (Sani et al., 2022).

Economic Sanctions and International Restrictions Scenario

Economic sanctions may restrict access to raw materials or critical equipment in the defense supply chain. This scenario examines the effects of sanctions and international restrictions on the capacity to supply military materials and equipment. Resilience strategies include diversification of suppliers, development of domestic production capabilities, and creation of strategic reserves of vital materials (Parvin, 2019).

Sudden Demand Change Scenario

Unexpected shifts in demand for weapons and military equipment can strain the defense supply chain. This scenario considers sudden changes in requirements for military resources and equipment. Resilience entails the ability to rapidly adapt to demand fluctuations, expand production capacity, and swiftly distribute equipment to military forces (Sani et al., 2022).

Research Methodology

This study is of an applied-developmental type, conducted with the aim of evaluating and analyzing the resilience of the defense supply chain in the face of various threats. The research adopts a quantitative approach, employing simulation as the primary method for modeling and analysis. The data were obtained through the simulation of processes and scenarios within the defense supply chain using statistical distributions. Additionally, data collection was supported by library sources and field information derived from existing data in the defense supply chain.

Research Instruments

For the simulations, the Simmer package in the R environment was utilized. Simmer is a discrete-event simulation framework developed in R. With its efficient and flexible simulation engine, it allows the modeling of complex and diverse processes. Simmer is particularly well-suited for modeling supply chain systems and logistics processes, enabling researchers to easily define and analyze different scenarios. In this study, Simmer was employed to model various resources of the defense supply chain (including suppliers, manufacturers, warehouses, and transportation) and to simulate different wargaming scenarios.

For data analysis and visualization, the ggplot2 and dplyr packages were used. **ggplot2** is a powerful package for generating graphs and statistical charts in the R environment. Based on the grammar of graphics, it enables researchers to easily produce complex and customized plots. In this research, ggplot2 was used to create charts illustrating the utilization of resources and the scheduling of processes throughout the simulations. These visualizations enhance the comprehensibility of the impacts of various scenarios on supply chain performance. **dplyr** is a package designed for data processing in R, offering functionalities such as filtering, sorting, grouping, and summarizing data. It is particularly effective for managing and analyzing large and complex datasets. In this study, dplyr was employed to process and summarize data generated by the simulations, allowing analysts to evaluate results effectively and accurately.

Simulation Model Design

In simulating the defense supply chain, the precise design of the simulation model plays a critical role. The model must be structured to comprehensively cover all dimensions of the supply chain, including suppliers, manufacturers, warehouses, and transportation systems. The primary objective of this model is to analyze and evaluate the resilience of the supply chain when confronted with threats and critical scenarios such as cyberattacks, logistics delays, equipment failures, physical threats, natural disasters, economic sanctions, and sudden changes in demand. These scenarios were modeled using the wargaming approach, and the performance and resilience of each segment of the supply chain were evaluated separately.

At this stage of the study, the key resources and processes of the defense supply chain were defined in accordance with their actual capacities and constraints, after which critical scenarios were simulated to examine the response of the defense supply chain to these threats.

Resource Definition:

Multiple resources were defined within the defense supply chain, including suppliers, manufacturers, warehouses, and transportation. Each resource was modeled according to its real capacities and limitations:

- **Suppliers**: Provide raw materials and essential equipment.
- **Manufacturers**: Carry out production processes.
- **Warehouses**: Store materials and products.
- **Transportation**: Responsible for moving materials and products.

Process Definition

Three main processes were defined in the defense supply chain, including raw material acquisition, production, and distribution to customers. Each process was modeled with respect to the resources involved and the associated time requirements:

- **Raw Material Acquisition**: Procuring materials from suppliers, transporting them to warehouses, and storing them.
- **Production Process**: Retrieving materials from warehouses, producing goods, and returning products to warehouses.
- **Distribution to Customers**: Retrieving products from warehouses, transporting them to customers, and delivering them.

Definition of Critical Scenarios

To assess the resilience of the defense supply chain, seven wargaming scenarios were defined, including cyberattacks, logistics delays, equipment failures, physical threats, natural disasters, economic sanctions, and sudden demand fluctuations. Each of these scenarios leads to disruptions in different processes of the defense supply chain, and their effects on performance and resilience are evaluated:

- **Cyberattack**: Cyberattacks disrupt the information systems of the defense supply chain, causing delays in coordination, information transfer, and critical operations. Resilience depends on cybersecurity and preparedness against such attacks.

- **Logistics Delay**: Transportation and coordination problems may delay the delivery of military equipment. Resilience requires improved transportation systems and contingency planning.
- **Equipment Failure**: Failures in production or logistics equipment can disrupt the defense supply chain. Resilience improves through preventive maintenance and equipment monitoring systems.
- **Physical Threats**: Terrorist attacks or sabotage can target critical infrastructure. Physical security and emergency programs are essential for countering these threats.
- **Natural Disasters**: Natural calamities can disrupt military production and transportation. Resilience requires robust infrastructure and rapid recovery programs.
- **Economic Sanctions**: Sanctions restrict access to vital resources. Diversification of supply sources and strategic reserves are necessary.
- **Sudden Demand Fluctuations**: Unexpected increases or decreases in demand impose pressure on the defense supply chain. Rapid adaptability and capacity expansion are key to resilience.

Simulation Design

Simulation, as a powerful tool for evaluating and analyzing complex systems, was employed in this research to investigate the resilience of the defense supply chain. The simulation was designed by integrating defined processes with wargaming scenarios to assess the impacts of diverse threats on defense supply chain performance.

Simulation Execution

The simulation was executed by combining the defined processes with the wargaming scenarios. It was conducted over a period of **250 days** to examine the impacts of each scenario on the performance and resilience of the defense supply chain.

Resources, Entities, and Constraints in the Simulation

In the resilience simulation of the defense supply chain, multiple resources, entities, and constraints were utilized, each fulfilling a specific role within the process. The following table presents the number and roles of the resources employed in the simulation. The column “Frequency” indicates the number of times each resource was used during the

simulation. These resources were applied across different processes to evaluate supply chain performance under varying conditions.

Table 1. Resources Employed in the Simulation

Resource	Quantity	Role
Supplier 1	3	Provision of raw materials from suppliers and their transfer to warehouses.
Supplier 2	2	Support of procurement processes and delivery of materials.
Manufacturer	4	Conversion of raw materials into final products and management of production processes.
Warehouse	5	Storage of raw materials and final products for distribution to customers.
Transportation	3	Transport of raw materials and products between suppliers, manufacturers, and warehouses.

Entities Employed in the Simulation

In the simulation of defense supply chain resilience, various entities have been incorporated, each playing a specific role in the defense supply chain process. The number of these entities was selected to adequately replicate the real conditions of the supply chain.

Table 2. Entities Employed in the Simulation

Entity	Quantity	Role
Receiving unit	7	Receipt of raw materials from suppliers and their transfer to warehouses.
Production unit	7	Transformation of raw materials into final products using production equipment and resources.
Delivery unit	7	Delivery of final products to customers and transfer from warehouse to final destination.

Critical Scenarios Employed in the Simulation

In addition to entities that operate within the defense supply chain, the simulation also modeled obstacles and threats that influence its performance. These threats were designed using war-game scenarios and directly impact different processes of the defense supply chain.

Table 3. Critical Scenarios Employed in the Simulation

Threat	Quantity	Role
Cyber-attack	3	Disruption of information and communication systems in the defense supply chain, leading to delays in coordination and data transfer.
Logistics delay	3	Transportation issues, lack of coordination across units, and delays in delivery of equipment and resources.
Equipment failure	3	Disruption of production due to malfunction of machinery or critical equipment in arms factories and warehouses.
Physical threat	3	Physical attacks such as terrorism or sabotage that may result in the destruction of key facilities and infrastructure.
Natural crises	3	Natural disasters such as earthquakes and floods that may interrupt production and transportation of military equipment.
Economic sanctions	3	Restriction in access to vital raw materials and equipment due to international sanctions.
Sudden demand changes	3	Abrupt fluctuations in demand for military equipment, placing pressure on the defense supply chain and causing disruptions in production and distribution processes.

Process Times

The durations of processes such as receiving, production, and delivery of products were generated randomly using the exponential distribution. The exponential distribution is particularly suited for simulating inter-event times in stochastic processes, as real-world intervals between two events are typically unpredictable. For example, the time required to receive raw materials from suppliers or to produce a final product may vary depending on operational conditions, and the exponential distribution appropriately models such uncertainties. Given its alignment with real-world processes such as random inter-arrival and response times, the exponential distribution is well-suited for simulating the defense supply chain. It is particularly relevant when inter-event times follow a constant hazard rate.

Resource Capacities

The capacities of different resources—including suppliers, manufacturers, warehouses, and transportation vehicles—were defined as fixed, based on the specific conditions of the defense supply chain. For instance, the number of machines or transport vehicles in each part of the supply chain was set as constant. These capacities were manually determined in accordance with system characteristics and the scale of activities. The assumption of fixed capacities in the simulation was made

because, in defense supply chains, such values generally remain stable within a defined time frame and depend on internal organizational factors and existing infrastructure. Fixed capacities allow for more precise assessment of system resilience under external changes and stress induced by threats.

Critical War-Game Scenarios

War-game scenarios—including cyber-attacks, logistics delays, equipment failures, physical threats, natural crises, economic sanctions, and sudden changes in demand—were modeled using different probability distributions and generated periodically. Each scenario was assigned specific time intervals during which it occurs. The use of probabilistic distributions was intended to reflect the stochastic and unexpected nature of these threats, which may impose sudden and severe disruptions on the defense supply chain. Periodic and random implementation of these scenarios enhanced the realism of crisis conditions in the simulation, thereby enabling the system to demonstrate its resilience under practical conditions.

Defense Supply Chain Resilience Strategies

To enhance the resilience of the defense supply chain against critical scenarios, specialized and targeted strategies must be employed to mitigate the impact of each threat and strengthen the system's capacity to withstand them. These strategies, grounded in literature review and recommendations from logistics experts and professionals, are outlined below:

Economic sanctions:

- Diversification of resource supply: By strengthening domestic and international procurement networks and employing multiple, sustainable suppliers, dependency on specific sources is reduced and resilience is improved.
- Enhancement of domestic production capacity: Developing advanced domestic production technologies and leveraging national technical expertise reduces reliance on imported raw materials and equipment.
- Strategic stockpiling of essential goods: Maintaining strategic reserves of vital materials in secure locations enhances the supply chain's ability to withstand sanctions.

Equipment failure:

- Predictive and preventive maintenance: Using intelligent systems and advanced data analytics for fault prediction reduces downtime and enhances supply chain efficiency.
- Advanced monitoring: Continuous monitoring and real-time data analysis of equipment status minimize reaction time to failures.
- Rapid equipment replacement protocols: Establishing spare-parts supply networks and expedited replacement procedures reduces downtime and disruptions.

Logistics delays:

- Optimization of transport routes: Employing intelligent algorithms and dynamic routing maps ensures the fastest possible transport routes, minimizing delays.
- Predictive and risk management systems: Artificial intelligence can forecast logistic risks and propose alternative routes and rapid responses.
- Development of logistics infrastructure: Strengthening military and logistic transport infrastructure and creating new arteries increase supply chain speed and efficiency.

Cyber-attacks:

- Strengthening cybersecurity: Implementation of advanced security protocols and robust encryption systems is essential for safeguarding defense digital infrastructures.
- Staff training: Continuous training programs for staff to recognize and counter cyber threats enhance system security.
- Backup and recovery systems: Establishing redundant systems and rapid data recovery mechanisms reduces response time to cyber incidents.

Physical threats:

- Enhanced physical security surveillance: Deployment of advanced monitoring systems and reinforcement of physical security in key facilities is crucial.
- Development of resilient infrastructure: Designing secure and durable structures against physical threats and natural disasters minimizes potential damages.
- Early warning systems: Installation of immediate alert systems improves response time in the event of physical threats.

Sudden demand fluctuations:

- Accurate demand forecasting: Advanced forecasting tools and demand modeling based on historical data enable effective management of abrupt demand changes.
- Flexible production systems: Adaptive production systems with rapid scaling capacity support the supply chain in managing demand volatility.

Natural crises:

- Crisis management programs: Comprehensive contingency plans for rapid response and recovery after natural disasters reduce disruptions.
- Geographic distribution of facilities: Strategic dispersal of defense and logistics facilities in safe regions prevents concentrated vulnerabilities.
- Insurance coverage: Adequate insurance of critical facilities accelerates recovery following crises.

Research Findings

This section presents and analyzes the findings derived from the simulation of defense supply chain resilience under different war-game scenarios. For this purpose, various models of defense supply chain processes—including receiving, production, and product delivery, along with cyber-attacks, logistics delays, equipment failures, physical threats, natural crises, economic sanctions, and sudden demand fluctuations—were designed and implemented.

Results of critical scenario simulations in the defense supply chain

Table 4 summarizes the simulation results, including the start time, end time, and duration of activities for each critical scenario.

Table 4. Results of Critical Scenario Simulations in the Defense Supply Chain: Start Time, End Time, and Duration

Scenario	Start Time	End Time	Activity Duration
Cyber Attack 1	50	77.47	27.47
Cyber Attack 2	100	102.85	2.85
Cyber Attack 3	150	154.82	4.82
Logistics Delay 1	60	98.10	38.10
Logistics Delay 2	120	130.26	10.26

Logistics Delay 3	180	191.40	11.40
Equipment Failure 1	70	111.17	41.17
Equipment Failure 2	140	204.73	64.73
Equipment Failure 3	210	221.41	11.41
Physical Threat 1	30	52.30	22.30
Physical Threat 2	90	100.09	10.09
Physical Threat 3	150	162.98	12.98
Natural Disaster 1	80	85.79	5.79
Natural Disaster 2	160	161.51	1.51
Natural Disaster 3	240	240.78	0.78
Economic Sanction 1	60	75.12	15.12
Economic Sanction 2	120	192.39	72.39
Economic Sanction 3	180	200.40	20.40
Sudden Change 1	40	65.15	25.15
Sudden Change 2	100	110.75	10.75
Sudden Change 3	160	164.93	4.93

Based on the results presented in the table above, economic sanctions rank as the foremost threat, as they can severely restrict access to resources necessary for production and distribution. Following this, equipment failures emerge as the second most significant threat, disrupting the supply chain due to technical malfunctions. Logistics delays also constitute another critical threat, disturbing transportation processes and hindering the timely distribution of resources.

Although threats such as cyberattacks and physical threats demonstrate shorter active durations, their indirect yet profound impacts on infrastructure and supply chain operations place them among the subsequent priorities. Sudden changes in demand and natural disasters also represent additional threats with comparatively limited effects, yet preparedness for managing them remains essential.

The interpretation of each scenario's results is as follows:

- **Economic sanctions**: With an active duration of 72.38 time units, this threat exhibits the longest duration. Sanctions can severely restrict the supply chain's ability to procure raw materials and essential components. Under sanction conditions, access to goods and services diminishes, leading to production difficulties that may disrupt the overall defensive performance of the country.

- **Equipment failures**: With an active duration of 64.73 time units, this threat is the second most significant factor within the supply chain. Failures in equipment, particularly in critical production and maintenance processes, can halt production lines and reduce the overall productivity of the supply chain. Such disruptions necessitate rapid repairs and technical support.
- **Logistics delays**: With 38.09 time units, logistics delays have a considerable effect on the delivery of goods and resources to their destinations. Transport delays create coordination gaps across different parts of the supply chain, leading to reduced efficiency and performance.
- **Cyberattacks**: With 27.47 time units, this threat highlights that attacks on the information and digital infrastructures of the defense supply chain can seriously disrupt operations. Loss of access to reliable data and attacks on digital systems can slow response times and impair decision-making.
- **Physical threats**: With 22.30 time units, physical threats can directly damage key facilities and infrastructure in the supply chain. These threats require robust physical security and continuous monitoring to mitigate risks.
- **Sudden changes in demand**: With 25.15 time units, this factor generates fluctuations in the production and distribution of resources. Misalignment between supply and demand may cause storage and distribution challenges, placing pressure on the supply chain.
- **Natural disasters**: With an active duration of 5.79 time units, natural disasters pose the least threat. Nonetheless, the supply chain must prepare for natural hazards such as earthquakes, floods, and severe storms to minimize disruptions.

Analysis of Simulation Results on Activity Durations

In Figure 1, based on the simulation data, the horizontal axis (x) represents the end time of activities, while the vertical axis (y) denotes the duration of each activity. Colors distinguish each entity or scenario, and each point represents a specific activity completed by an entity at a given time.

Interpretation of the figure:

- **Diversity in activity durations**: The points along the vertical axis indicate that some entities had longer-lasting activities compared to

others. For example, entities such as equipment failure and logistics delay exhibited prolonged activities, reflecting higher complexity and a more substantial effect of these scenarios on the supply chain's performance.

- **End times of activities**: The distribution of points on the horizontal axis shows that some activities concluded quickly, while others lasted longer. For instance, scenarios such as natural disasters and equipment failures occurred in the latter stages of the simulation period, exerting their influence during the final phases.

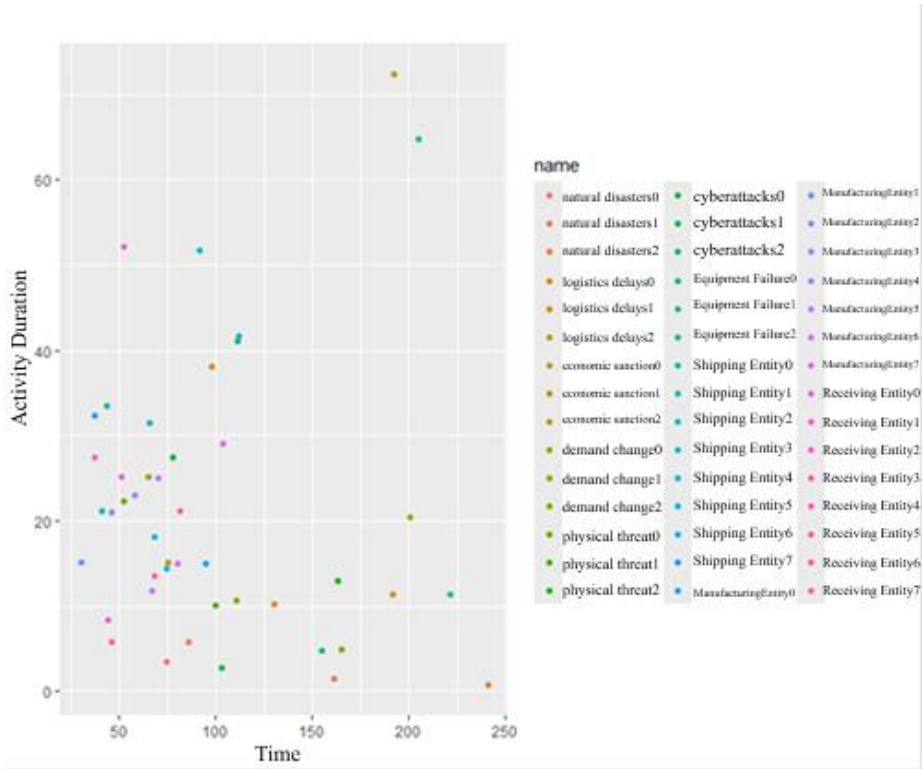

Figure 1: Activity durations in the defense supply chain

- **Entities with extended activities**: Specifically, the entities related to transportation and production displayed long-term activities, indicating the complexities and interdependencies within the defense supply chain. Additionally, equipment failures and logistics delays prolonged activity durations due to breakdowns or disruptions in transportation.

- **Key points in activities**: Certain activities, such as those related to cyberattacks and economic sanctions, stand out for their pronounced effects at various points in time, highlighting the sudden and disruptive nature of these scenarios on the defense supply chain.

Overall, the figure illustrates that the defense supply chain is subject to diverse interferences and delays under various scenarios. Each entity responds differently to these impacts, with activities ending at different times during the simulation. Scenarios such as equipment failure, logistics delay, and cyberattack were identified as primary factors influencing the duration of key defense supply chain activities.

Analysis of Resource Utilization Trends Over Time

Figure 2 effectively depicts the fluctuations and variations in the utilization of key resources within the defense supply chain over time. The dynamic use of resources reveals that challenges and different scenarios exert direct effects on capacity and resource exploitation. Peaks in resource utilization highlight critical moments that necessitate improved resource management and capacity-building to enhance the resilience of the defense supply chain.

The horizontal axis (x) represents time, while the vertical axis (y) indicates the number of servers or capacity utilized per resource. Colors distinguish the various resources employed in the simulation, including Supplier 1, transportation, warehouse, production, and Supplier 2.

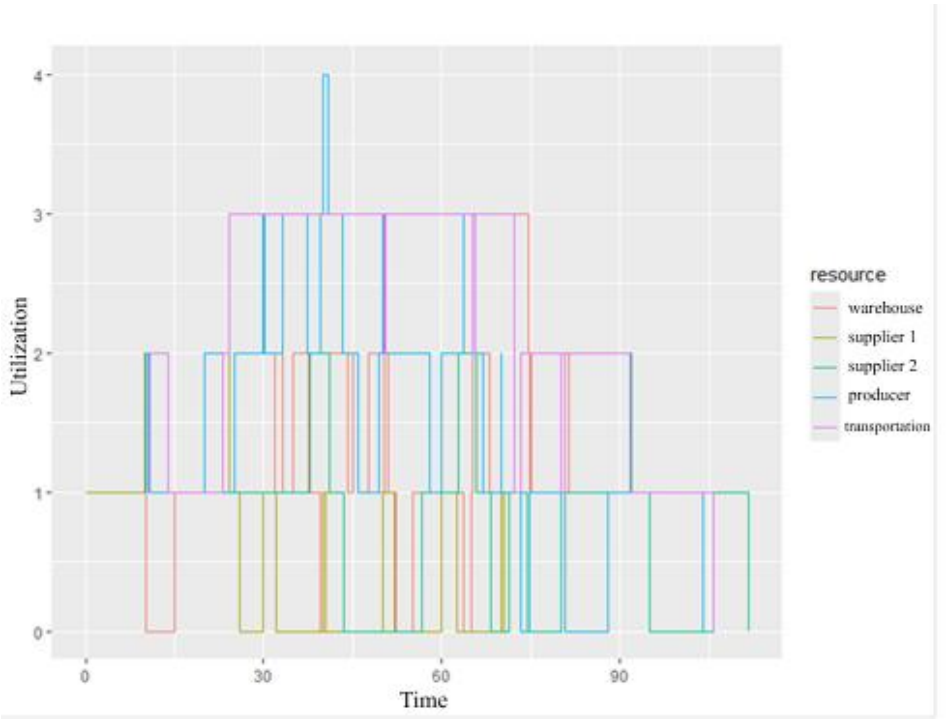

Figure 2: Utilization of Defense Supply Chain Resources Over Time

Fluctuations in Resource Utilization: The chart, presented as a step line graph, illustrates the periodic variations in the usage of each resource. For instance, certain resources may experience higher pressure during specific intervals (high capacity utilization) and subsequently show reduced usage at other times. These fluctuations reflect the dynamic consumption of resources throughout various activities in the defense supply chain.

Critical Points and Peak Utilization: Some resources, such as transportation and Supplier 1, were heavily utilized during specific periods of the simulation. Notably, the higher steps in server utilization indicate peak activity points in the defense supply chain, where resources approached their maximum capacity. These conditions may arise due to scenarios such as cyberattacks, logistics delays, or equipment failures, which place additional pressure on key resources.

Analysis of the Impact of Implementing Proposed Strategies on Defense Supply Chain Resilience

Following the implementation of the proposed strategies, simulation parameters were updated to assess the potential effects of these improvements on the resilience of the defense supply chain. Experts in the field provided their evaluations regarding the effectiveness of the proposed strategies, and the results of the updated simulations are presented in the following chart.

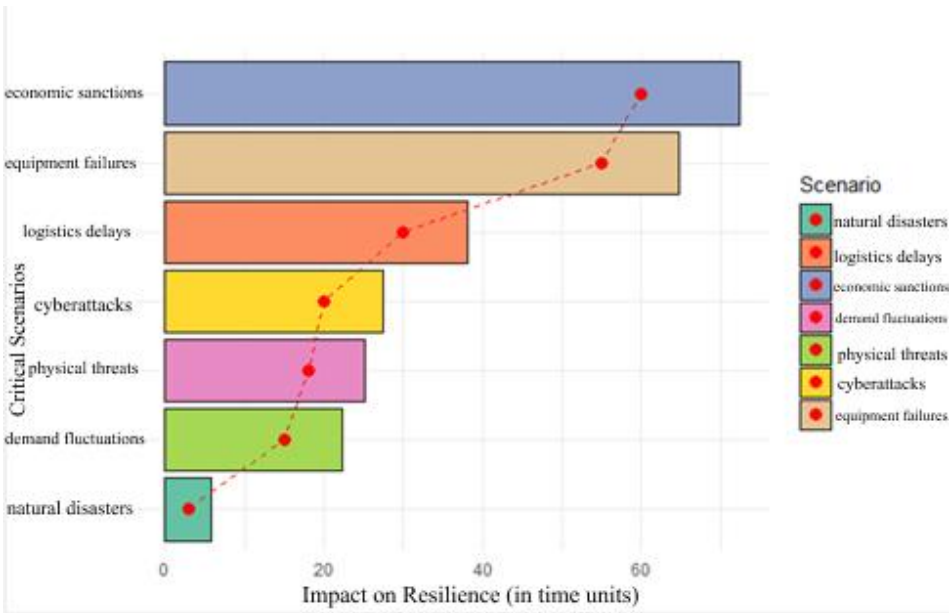

Figure 3: Impact of Critical Scenarios on the Defense Supply Chain and Reduction of Duration Following Strategy Implementation

Figure 3 illustrates the influence of critical scenarios on the resilience of the defense supply chain and shows how the duration of each scenario decreased after implementing various strategies. The vertical axis (y) represents the critical scenarios affecting the defense supply chain, while the horizontal axis (x) shows the impact of these scenarios on resilience (in time units). Colored bars indicate the extent of each scenario's impact prior to strategy implementation, and red points along with dashed lines depict the reduction in duration and improvement in resilience following the strategies. Detailed interpretation of the chart is as follows:

Economic Sanctions: This scenario has the greatest impact on defense supply chain resilience (72.39 time units). After implementing strategies related to resource diversification and strategic reserves, the impact decreased to 60 time units, demonstrating a significant improvement in resilience.

Equipment Failures: With an impact of 64.73 time units, this is the second most critical scenario. Preventive maintenance and advanced monitoring strategies reduced the duration to 55 time units.

Logistics Delays: With an impact of 38.10 time units, strategies such as route optimization and anticipation of logistics risks reduced the scenario duration to 30 time units.

Cyberattacks: With an impact of 27.47 time units, implementing cybersecurity measures and employee training decreased the duration to 20 time units, indicating a reduced effect of cyberattacks on the defense supply chain.

Physical Threats: The impact of these threats is 22.30 time units, but increasing security monitoring and enhancing physical resilience of facilities reduced it to 15 time units.

Demand Fluctuations: Sudden changes in demand have an impact of 25.15 time units. By employing precise forecasting strategies and production flexibility, this duration was reduced to 18 time units.

Natural Disasters: This scenario has the least impact (5.79 time units). After implementing crisis management strategies and geographically dispersing facilities, the duration was reduced to 3 time units, demonstrating improved resilience in response to natural crises.

Conclusions and Recommendations

Conclusions

This study aimed to enhance the resilience of the defense supply chain against various critical scenarios by employing simulation methods and war game scenarios. Given the strategic importance of the defense supply chain in maintaining national security and the operational capabilities of armed forces, it is essential that these supply chains remain resilient and logistics-ready against diverse threats that could disrupt their functionality.

Simulation results indicated that economic sanctions exert the most significant influence on the defense supply chain, potentially disrupting the supply of raw materials and critical equipment. Equipment failures emerged as the second major threat, capable of causing production line shutdowns and reducing operational efficiency. Additionally, logistics delays, cyberattacks, physical threats, sudden demand changes, and natural crises all had varying impacts on defense supply chain resilience.

The implementation of the proposed strategies, including resource diversification, strengthening domestic production capacity, improving logistics infrastructure, and enhancing cybersecurity, significantly reduced the disruption duration for each critical scenario. These improvements demonstrate that preventive measures and process optimization can substantially enhance defense supply chain resilience.

Recommendations

1. **Diversification of Supply Sources and Strengthening Domestic Production Capacity:** To counter economic sanctions, establishing multiple supply networks and enhancing domestic production capabilities is critical. It is recommended to reduce reliance on foreign suppliers and adopt advanced technologies to expand domestic production capacity.
2. **Preventive Maintenance:** To mitigate equipment failure impacts, implementing preventive maintenance programs and utilizing advanced monitoring systems is advised. Such strategies can prevent sudden breakdowns and reduce response times to equipment failures.
3. **Optimization of Transportation Routes and Logistics Infrastructure:** To minimize the effects of logistics delays, employing intelligent algorithms for route optimization and developing logistics infrastructure is essential. These strategies can enhance the speed and efficiency of logistics processes, reducing delays.
4. **Enhanced Cybersecurity and Staff Training:** To counter cyberattacks, establishing advanced cybersecurity protocols and increasing employee awareness regarding cyber threats is essential. Additionally, developing information support and recovery systems can shorten response times to such threats.
5. **Strengthening Physical and Security Infrastructure:** To reduce the impact of physical threats, developing facilities resistant to

physical attacks and natural disasters, along with enhancing security monitoring, is necessary.

6. **Forecasting and Managing Demand Changes:** To address sudden demand fluctuations, implementing precise demand forecasting models and flexible production processes is recommended. Flexible production enables the defense supply chain to respond rapidly to demand variations.
7. **Comprehensive Crisis Management Programs:** To mitigate the effects of natural disasters, developing and implementing crisis management plans and geographically dispersing facilities are proposed as key strategies. These approaches protect facilities and defense resources and facilitate rapid recovery following crises.

References

1. Yamini, Seyed Mohammad Hassan; Kazerooni, Hanif; Tabatabaei, Seyed Morteza; Rezaei. (2023). Formulation of a Resilience Calculation Model in the Defense Supply Chain. Logistics and Defense Technology Quarterly, 7(2), 11-46.
2. Rahimi, Rad; Abbas, Alam Tabriz; Motameni. (2018). Development of an Interpretive Structural Model for Resilient Supply Chains in Iran's Defense Industries. Military Management Quarterly, 18(71), 31-70.
3. Lucas, R., Ekström, T., Fusaro, P., Hastings Roer, E., & Retter, L. (2024). Toward Defense Supply Chain Disruption Management: A Research Agenda for Defense Supply Chain Resilience.
4. Urmston, A., Song, D., & Lyons, A. (2024). The Development of Risk Assessments and Supplier Resilience Models for Military Industrial Supply Chains Considering Rare Disruptions. Logistics, 8(2), 57.
5. Mustafee, N., Katsaliaki, K., & Taylor, S. J. (2021). Distributed Approaches to Supply Chain Simulation: A Review. ACM Transactions on Modeling and Computer Simulation (TOMACS), 31(4), 1-31.
6. Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. The international journal of logistics management, 20(1), 124-143.

7. Chopra, S., & Meindl, P. (2016). "Supply Chain Management: Strategy, Planning, and Operation." Pearson.
8. Ekström, T., Hilletofth, P., & Skoglund, P. (2020). Differentiation strategies for defence supply chain design. Journal of Defense Analytics and Logistics, 4(2), 183-202.
9. Sabin, P. (2012). Simulating war: Studying conflict through simulation games. Bloomsbury Publishing.
10. Zhao, Y., Hemberg, E., Derbinsky, N., Mata, G., & O'Reilly, U. M. (2021, July). Simulating a logistics enterprise using an asymmetrical wargame simulation with soar reinforcement learning and coevolutionary algorithms. In Proceedings of the Genetic and Evolutionary Computation Conference Companion (pp. 1907-1915).
11. Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. International Journal of Production Research, 60(1), 162-183.
12. Coyle, J. J., Novack, R. A., Gibson, B. J., & Langley, C. J. (2021). Supply chain management: a logistics perspective. Cengage Learning.
13. DeBerry, W. T., Dill, R., Hopkinson, K., Hodson, D. D., & Grimaila, M. (2024). The wargame commodity course of action automated analysis method. The Journal of Defense Modeling and Simulation, 21(1), 17-29.
14. Adenekan, O. A., Ezeigweneme, C., & Chukwurah, E. G. (2024). Strategies for protecting IT supply chains against cybersecurity threats. International Journal of Management & Entrepreneurship Research, 6(5), 1598-1606.
15. Sani, S., Schaefer, D., & Milisavljevic-Syed, J. (2022). Strategies for achieving pre-emptive resilience in military supply chains. Procedia CIRP, 107, 1526-1532.
16. Praveen, A. (2019). Adaption Strategies For Supply Chain Recovery during Economic Sanctions (Doctoral dissertation, Curtin University).