SUPPLY CHAIN RISKS AND MANAGEMENT STRATEGIES IN THE DEFENSE INDUSTRY

Goksel KORKMAZ, PhD

Ministry of National Defense, Turkiye

This study aims to explore the risks within the defense industry supply chain—a realm with limited existing research. The focus is on understanding these risks, their potential impacts, and evaluating mitigation measures and risk management strategies. The examination encompasses various facets of supply chain risks, categorizing them into supplier-related risks, risks stemming from globalization and foreign dependency, sector-specific risks, and cyber security risks. The study delves into the effects of these risks specifically within the defense industry context. Notably, it also presents actionable measures and determinations related to risk management strategies. The primary contribution of this study lies in providing a comprehensive framework for managing risks within the defense supply chain, emphasizing the "how" rather than just the "what."

Key words: *Supply chain risks, supplier risks, foreign dependency, defense sector, defense acquisition.*

1. INTRODUCTION

Resource-based theory suggests that the success of businesses is contingent upon three types of resources: physical, human, and organizational capital. However, for these resources to confer a competitive advantage, they must possess characteristics such as being valuable, rare, inimitable, superior, and organized systematically (Barney, 1991). Additionally, the capabilities of an institution serve as a complementary element to its resources and are crucial in explaining variations in performance, even when resources are identical (Gunasekaran et al., 2017). On the contrary, an alternative perspective posits that the primary variable influencing an institution's success is the dynamics of the industry in which it operates (Porter, 1981). Indeed, a more comprehensive understanding may be that both viewpoints are complementary, as organizations must align their resources and capabilities with the specific needs of their industry (Gellweiler, 2018). Effectively managing supply chain risks in accordance with physical, human, and organizational resources, as well as industry dynamics, can be

considered a vital capability for corporate competition and sustainability (Srivastava and Rogers, 2021: 3).

Supply chain management involves overseeing the material, information, financial flows, and network of relationships between independent organizations—from suppliers to end customers, in both forward and backward directions—with the aim of maximizing profits and customer satisfaction (Stock and Boyer, 2009). Presently, organizations increasingly rely on suppliers to support critical functions, a trend that has significantly accelerated in the last decade and is expected to continue due to factors such as globalization, outsourcing, and digitalization. The interconnected nature of supply chains, where suppliers have their own suppliers, exposes these networks to various threats, including cyber threats and external disruptions like severe weather and geopolitical unrest. Consequently, the significance of supply chain resilience, business continuity, and disaster recovery planning has risen (NIST, 2020). Inability to effectively address supply chain risks leads to disruptions in business operations. While past supply chain management focused on cost reduction, affordable procurement, and inventory management improvement, the current landscape emphasizes the importance of supply chain sustainability for overall business success (Samvedi et al., 2013).

Post-COVID-19 global risk studies consistently highlight supply chain risks among the most critical. For instance, in a survey by Allianz of nearly 2,800 businesses across 92 countries, business interruption due to supply chain disruptions emerged as the foremost risk, with 94% of businesses reporting such interruptions in 2020 (Gosh, 2021). Supply chains are only as robust as their weakest link; hence, as the chain expands, its susceptibility increases. Presently, global supply chains grapple with significant disruptions affecting the container market, shipping routes, ports, airlines, truck lines, railways, and even warehouses. These disruptions lead to shortages in crucial production components, order backlogs, delivery delays, increased transportation costs, and higher consumer prices. If the situation is not rectified promptly, the conseqauences for the global economy could be severe (Friesen, 2021). Adapting to today's dynamic environment and responding swiftly to changes necessitates the design, development, and maintenance of a flexible supply chain. Globalization, shorter product life cycles, intricate trade partnerships spanning numerous countries, market demand uncertainties, cost pressures, outsourcing, and offshoring represent

significant sources of supply chain risk (Hachicha and Elmsalmi, 2014: 1308). The escalating complexity of supply chains corresponds with an increase in uncertainty and risk (Sofyalıoglu and Kartal, 2012: 1450). Supply chain risk, defined as the potential for a negative and unforeseen event directly or indirectly leading to supply chain interruption, underscores the importance of effective risk management (Garvey et al., 2015: 620). Unforeseen risks emanating from the supply chain can render it vulnerable. The ongoing impact of the recent pandemic has significantly disrupted supply chains across various sectors, particularly in the production sector (Haren and Simchi-Levi, 2020).

Previous studies indicate that distinct sectors should emphasize varied supply chain risk management strategies (Rajesh and Ravi, 2015; Tse et al., 2016). For instance, companies in the food industry will need to tailor their risk management practices differently compared to those in the fashion industry, as both face different types and levels of environmental dynamism. Specifically, firms operating in industries characterized by uncertainty and resource scarcity encounter different risks than those in more stable and resource-rich sectors. Consequently, the nature of risks and the practices for their management will significantly differ (Beske et al., 2014; Darby et al., 2020).

However, existing empirical evidence exploring suitable supply chain risk management strategies at the industry level falls short in providing adequate data explaining why certain risk management strategies prove effective in one industry sector but not in another. The global disruption caused by the COVID-19 pandemic serves as a pertinent example of how supply chain risk exposure and severity vary across industry types (Srivastava and Rogers, 2021: 2). COVID-19 has triggered a ripple effect across supply chains in various industries, placing them under unprecedented pressure. The imposition of quarantine measures worldwide has led to significant restrictions on the free movement of goods, creating a situation unlike any other in the past. In certain industries, lockdowns resulted in the suspension of raw material movements, causing substantial challenges for companies, suppliers, and logistics departments. The combination of decreased supply and relatively unchanged demand has led to significant price increases. Today's supply chains, characterized by their size, dynamic nature, complexity, and the escalating demands and expectations of customers, are increasingly susceptible to disruptions (Son and

Orchard, 2013). Surprisingly, research indicates that only 10% of companies have comprehensive plans in place to mitigate potential disruptions in their supply chains (Black and Ray, 2011).

Dowdall contends that the defense industry supply chain has received less research attention compared to other supply chains, primarily due to the complexity of products, challenges in accessing data, and the intricacies of economic networks. The defense industry encompasses a diverse and dynamic array of companies, including both private entities and organic Department of Defense (DoD) facilities. These entities provide products and services directly or indirectly to the DoD and national security agencies in support of national security objectives. The defense sector, as a cornerstone of national security, experiences rapid changes in the supply chain ecosystem.

An additional factor that sets defense supply chains apart is their foundation on long-term cooperation. Given that the production of a defense system spans 5-10 years with an average lifespan of 50-60 years, businesses at each link in the supply chain of a defense system become part of a partnership that can endure for many years. The supply chain plays a pivotal role in the success of any defense organization. Effective and efficient supply chains empower these organizations to attain their strategic and financial objectives. Managing supply chain risks and adapting to emerging trends such as digital advancement and sustainability will be crucial for a sustainable future in the defense industry (E&Y, 2021).

In a risk analysis by E&Y on the world's 15 largest defense industry companies, supply chain-related risks ranked second among the ten most significant risks. Defense industry companies rely on numerous suppliers or subcontractors for raw materials, semi-finished products, or spare parts. The ability to meet quality standards, product specifications, and delivery times hinges on their relationships with these suppliers. Consequently, the supply chain emerges as the key to success for every institution, and achieving targets on time relies on the effective management of this network (E&Y, 2017).

In summary, the proliferation of global supply networks, coupled with current research findings, underscores the imperative to develop resilient supply chains capable of responding to disruptions and swiftly restoring supply chain operations to their original or improved state (Chang et al., 2015: 648).

2. RESEARCH AND FINDINGS

2.1. Possible Risks and Effects in Defense Supply Chains

Given the paramount importance of supply chain effectiveness in creating a competitive advantage, the shift in competition has transitioned from inter-organizational to inter-supply chain competition (Cabral et al., 2012: 4835). Effective supply chain management has evolved into a critical factor for organizational survival, becoming an integral component of any business. Proficient supply chain management has the potential to enhance customer service, reduce operating costs, improve product quality, and accelerate delivery and innovation (Li et al., 2006: 110). Consequently, supply chain-related risks are imperative to be effectively managed by organizations.

While increased globalization of defense supply chains may offer cost benefits, it simultaneously introduces complexity, compounded by the numerous relationships within these chains and their intricate, interdependent layered nature. For instance, an engine manufacturer, a crucial member of the overall production supply chain in the defense industry, relies on its own supply chain for engine production. The existence of multiple layers of supply chains within the system complicates both the complexity and manageability of the entire network (E&Y, 2021).

In their study compiling supply chain risks specific to various industries, Srivastava and Rogers encompass risks in sectors such as automotive, construction, electronics, fashion, food, pharmaceuticals, energy, mining, and aviation. Among these, aviation risks, which bear resemblance to the defense sector, include challenges such as global resource fluctuations, variable market conditions, product complexity, and a diverse supplier base. In the automotive industry, risks involve supplier failure, supplier quality problems, oil crises, terrorist attacks, strikes, IT system failures, increased customs duties, changes in customer demand, technological advancements, and rising raw material prices (Srivastava and Rogers, 2021: 5).

The US Department of Defense identifies ten risks threatening the defense industry in its report, encompassing issues like a single resource for required talent, fragile suppliers and markets, capacity-constrained supply markets, foreign dependencies, decreasing manufacturing resources, material scarcity, gaps in US-based manpower capital, erosion in defense infrastructure, and product security risks (DoD, 2018: 30-55). RAND Corp.'s 2015 research on supply

chain risks in the US Army and Air Forces highlights the three most significant risks as fluctuations in demand, uncertainties about financing, and extended delivery times due to administrative or production reasons (RAND, 2015: 14).

A 2018 study by E&Y identifies key risks including dependency on a single source, long delivery times, financial difficulties, inventory density, collaboration management throughout the supply chain, and cyber threats (E&Y, 2018: 5). Pre- and post-COVID-19 studies on supply chains exhibit notable differences. While epidemic or disaster risks were considered among the top ten supply chain risks in studies conducted before COVID-19, they took precedence in studies conducted afterward. The disruptions caused by the epidemic exceeded calculated possibilities. A supply chain risks report presented to the US Senate emphasizes that the supply chain weakened by COVID-19 poses a threat to US national security. Excessive reliance on China in critical supply chains, particularly in the defense sector, presents significant strategic and competitive risks for the USA, allowing China to potentially impede the export of these products (HASC, 2021). Research conducted in England identifies six primary risks associated with defense industry supply chains. These include challenges faced by Small and Medium-sized Enterprises (SMEs) and mid-level suppliers in accessing main contractors and the Ministry of Defense, a lack of innovation due to difficulties attracting non-traditional suppliers to the sector, hindrances posed by the durations and conditions of defense contracts on supply chain development, shortcomings in the critical defense industry workforce, and the industry's slower adoption of new production technologies compared to other sectors, coupled with its vulnerability to cyber threats (RAND, 2021).

Moreover, the impact of the Covid-19 pandemic has been felt in the UK, as in other countries. Defense supply chains encountered urgent difficulties in timely program delivery due to production delays and delayed payments to defense suppliers, resulting from disruptions caused by the pandemic (Lye, 2020). In light of the aforementioned considerations, risks pertaining to defense industry supply chains can be categorized under supplier-related risks, risks arising from globalization and foreign dependency, sector-specific risks, and cyber security risks.

2.1.1. Risks originating from suppliers

One of the most prevalent supplier-related risks is dependence on a single source, characterized by

non-competitive procurement negotiations with only one supplier. In an era of budget constraints and governments aiming to maximize efficiency with reduced spending, full and open competition is crucial for obtaining the best value for money. However, studies indicate a weakness in the defense sector regarding competitive procurement (Pyman et al., 2009: 216).

The risk associated with a single source extends both nationally and globally. As exemplified by the F-35 case, its global dimension is closely tied to international relations. This risk arises when a single company has the capacity to fulfill the required system/material/service requirements, and it stands out as one of the most common risks in the defense industry. The prevalence of single sourcing in various defense sectors exposes the industry to global and local supply shortages, diminishing readiness. The specialized nature of the industry, particularly in the aviation sector, impedes competition, hindering potential market entrants from benefiting from economies of scale enjoyed by established dominant vendors (Gonzalez and Rodriguez, 2021).

Relying on a dependable single-source supplier offers advantages such as ensuring quality, minimizing disruption risks, leveraging the brand value of a reputable supplier, building trust, and optimizing costs. However, any delay or quality issue at the sole-source supplier's end poses a heightened risk of production stoppage, delivery delays, and cost overruns (E&Y, 2018: 3). Being dependent on a single source in the defense industry also undermines risk management strategies, such as redundancy or diversification of the supplier base, which are among the most crucial approaches in supply chain management (Norris et al., 2020: 66).

Another supplier-related risk involves the use of unreliable imitations or poor-quality products, often sourced from subcontractors. Quality issues can even arise in globally monitored projects such as the F-35. For instance, out of over 10,000 critical manufacturing processes by airframe contractors, only 3,000 met predefined design standards on the F-35 project. Furthermore, the more than 500 aircraft in the field do not meet the program's reliability and maintainability goals. Although contractors are modifying production processes to address issues and enhance efficiency, there is acknowledgment that more needs to be done (GAO, 2020).

Counterfeit products are currently a major problem threatening the defense industry, with research indicating a significant portion originating from China. A study in

the USA in 2011, focusing on one million spare parts, revealed that 70% of them were traced back to China (Menz, 2018: 8). Recognizing this danger, Apple, as one of the companies vigilant against counterfeit products, has established a closed ecosystem to mitigate issues in the supply chain, especially those related to quality and faulty parts. Apple manages this closed ecosystem as an integrated process, intertwining all components, including production, purchasing, logistics, and suppliers. The company inspects the production lines of all its suppliers, emphasizing a holistic approach to supply chain management rather than treating it as an isolated application under the authority of a single department (Satariano, 2013). For the defense industry, imitation or counterfeit products not only pose significant security risks but also entail serious economic burdens for companies or the state. According to a 2012 report in the USA, the Missile Defense Agency and its contractors had to invest $4.5 million in reprocessing costs due to counterfeit products (Watson, 2015).

The defense industry grapples with fluctuating demand, at times leading to capacity risks. Many systems, especially those with a limited number of critical part manufacturers, face the potential of production interruptions due to these fluctuations. Increasing capacities necessitates additional investment, and the associated risks of fluctuating or interrupted demand post-investment also elevate the risk of return on investment (E&Y, 2018: 13). The combination of high production costs and the consolidation of the defense industry compels countries to increasingly prioritize readily available solutions in the international market rather than developing their own military equipment (Kluth, 2017: 160). However, imported technology must be adapted to align with the importing country's specific defense doctrines, infrastructures, and requirements.

For nations aspiring to maintain a domestic defense industry and critical technologies, two fundamental approaches address fluctuations in demand: dual production and export. Escalating defense system costs drive governments toward dependence on civilian or dual-use technologies and innovations within the defense industry (James, 2009: 450). Upon achieving the required number of systems, the production line should either be sustained with export connections or diversified by producing for needs outside the defense sector through dual production. Failure to effectively manage demand fluctuations may not only jeopardize individual businesses

but also impact all entities within the supply chain.

The defense industry, by its nature, necessitates the employment of a skilled and engineer-oriented workforce, along with qualified management personnel responsible for recruiting and overseeing them. This is due to the defense industry's involvement in complex production and system integration activities. Failure to attract and employ talented personnel, or the loss of existing personnel over time, can result in both cost and time losses and quality problems (Ernst & Young, 2018: 15). In the United States, a survey conducted in December 2017 of 662 manufacturing companies by the National Association of Manufacturers revealed that the primary business challenge, identified by 72.9% of respondents, was the inability to attract and retain a quality workforce. In response to this workforce challenge, 66% of respondents stated that they increased the workload of their current employees, while 34.4% mentioned that their companies were unable to secure new business opportunities and lost revenue due to challenges in attracting and retaining workers (Department of Defense, 2018: 50).

2.1.2. Risks resulting from globalization and foreign dependency

Similar to all sectors, the defense industry relies on various raw materials, intermediate products, and finished goods. These items can traverse international borders. However, unlike other sectors, such transactions in the defense industry can be significantly influenced by political fluctuations and international relations. For instance, diplomatic tensions between Japan and China in 2010 resulted in a de facto export ban on certain rare items to Japan. This raised concerns in Japan, which has limited natural resources and has long been apprehensive about import dependence (Bradsher, 2010). This situation prompted accusations against the Japanese government for inadequate investment in risk management (Inoue, 2010).

Another example occurred in the dispute between Turkey and the USA over the F-35 program. Following the US President's directive to exclude Turkey from the program, more than 900 parts of the F-35 were being produced in Turkey, with most in a single-source position (Clark, 2021). The decision to remove Turkey was estimated to cost 1 billion dollars, posing a significant risk for decision-makers. Despite political fluctuations, it was ultimately decided to continue purchasing these

spare parts from Turkey until 2022 (Sisk, 2020). However, the investments made by businesses in the supply chains of this multi-decade project in Turkey could pose a substantial risk post-2022.

The Covid-19 pandemic serves as a noteworthy example, revealing the risks foreign dependency may pose for the defense sector. During this period, some countries, similar to other sectors, experienced complete shutdowns in the defense industry, hindering the production of products required by other nations in the defense sector (Gould, 2020). Delays in the defense supply chain serve as a reminder to policymakers that offshore or foreign-dependent supply chains entail risks that may be unacceptable in the defense context (Clark, 2021). For instance, the United States relies entirely on imports for 19 minerals, and any disruption in the supply of these minerals could halt the production of defense systems such as radar and guided missiles (Humphries, 2015: 26). Seventeen of these minerals are sourced from China and find applications in other sectors of the economy, including high technology and clean energy (Symth, 2020). China, in turn, has the potential to blacklist companies or countries it deems harmful to its interests or connected to parties it perceives as harmful, particularly in the realm of rare earths (Gill and Pollard, 2020).

Similarly, the reliance on Japan and Europe as the only foreign sources of carbon fibers poses significant risks for the USA. Disruptions in the supply of carbon fibers could potentially impact the Ministry of Defense's missile, satellite, space launch, and other defense production programs. Often, there are no readily available substitutes for these materials, and establishing a new carbon fiber factory is both expensive and time-consuming. The uncertainty and substantial resource requirements for qualified replacement suppliers further compound this concern (Department of Defense, 2018: 49).

A critical issue regarding foreign dependency in defense supply chains is the need to balance cost-effective flow in peacetime with readiness and alternatives to ensure supply chain continuity during wartime. In peacetime, defense supply chains must meet usability and readiness requirements, while wartime demands focus on sustainability (Ekström et al., 2020: 186). According to Basnet and Seuring (2016), demand variability or uncertainty, product variety, desired customer delivery time, and supply uncertainty represent the fundamental conditions in supply chains, and these conditions will vary based on their state, whether it's peace, mobilization, or war. Transitioning from a state of peace to

a state of war, demand variability/uncertainty will shift from low to high, where desired delivery time and cost become more crucial, and, conversely, supply uncertainty/risk will increase during wartime. These defense-specific challenges need to be considered when formulating strategies for defense supply chains. In times of peace, supply chains should be simple and efficient, while in times of war, they should be agile and effective (Basnet and Seuring, 2016).

2.1.3. Risks arising from the sector (sector-specific)

The safety and security systems, as well as the quality assurance standards necessary for defense systems, demand suppliers to possess expertise and demonstrate maturity in these aspects. National security requirements might constrain the selection of specific suppliers or necessitate the use of designated suppliers, thereby limiting manufacturers' options and extending their supply chains. In this highly regulated industry, the entry of new suppliers may require substantial investments, potentially restricting market entry and leading to anti-competitive scenarios (Ernst & Young, 2021).

Another sector-specific challenge is the struggle to attract adequate investment from other sectors, leaving the field predominantly in the hands of traditional players and, consequently, constraining opportunities for innovation. For instance, a study on the defense industry in the UK indicates that defense procurement contracts and main contractor agreements involve slow, inflexible, and bureaucratic processes, adversely impacting contractors seeking entry into the sector. Non-traditional suppliers aiming to penetrate the defense market may need to make substantial investments, enhance the security standards of their products, invest in infrastructure security capacities, and restructure their processes. However, the return on these investments may not always justify the associated costs (RAND, 2021: 5).

Beyond sustainability concerns, the defense sector heavily relies on the commercial sector for technology advancement. However, the commercial sector, driven by revenue and high-volume technology demands, may not always prioritize the development of technology for military use (Department of Defense, 2018: 50).

2.1.4. Cybersecurity risks

The interconnectedness of computers through networks and the vast amount of information they contain have accelerated computing processes and brought the digital and physical worlds closer than ever before. While this approach enhances

efficiency, it also intensifies cyber threats. According to a study by the National Institute of Standards and Technology (NIST), 80% of all information breaches originate from the supply chain. Cyber supply chain risks encompass various threats, including the introduction of counterfeit products, unauthorized manufacturing, tampering, theft, insertion of malware and hardware, as well as substandard manufacturing and development practices in the cyber supply chain (NIST, 2020).

Moreover, recent reports indicate an escalating rate of attacks on supply chains. For instance, Symantec's research in 2019 revealed a 78% increase in supply chain attacks in 2018 (Davis, 2019). The concerning aspect of these attacks is their high success rate and the significant damage they inflict. A Ponemon Institute study in November 2018 found that 59% of organizations participating in the study experienced a data breach caused by one of their third parties (Ponemon and Opus, 2018). A survey by Crowdstrike in July 2018 further disclosed that 66% of respondents had encountered a software supply chain attack, with 90% of them experiencing financial impacts as a result, averaging over $1.1 million in cost per attack (Larson, 2018).

Supply chains in the defense industry are frequently targeted in cyber attacks due to their high priority and value as strategic assets for rival countries. As major companies enhance their cyber defenses, attack strategies have evolved from direct assaults on prime contractors to targeting other entities in the supply chain, including trusted vendors and subcontractors (Bluevoyant, 2021: 4). Notably, the Russian cyber attack group known as "Cozy Bear" successfully breached the data of over 18,000 organizations and clients through a cyber attack on the software company "Solarwinds," a subcontractor for numerous defense industry firms in the United States, exploiting its network monitoring platform "Orion" (Vavra and Starcks, 2020). A study by Bluevoyant focused on defense industry companies revealed intriguing findings. According to this research, the sector in which a company operates is more crucial than its size in determining the risk of cyber attacks, with the highest risk identified in Research and Development (R&D) companies. The size of the company, in conjunction with its field of activity, further amplifies this risk, indicating that small companies engaged in manufacturing and R&D are at significantly higher risk compared to counterparts in other size groups or sectors (Bluevoyant, 2021: 10). The defense supply chain, often containing state secrets, faces constant threats from external forces,

making its protection a national security priority (Norris et al., 2020).

Small and Medium-sized Enterprises (SMEs) form the backbone of the defense industry and bear significant responsibility. Operating on cash profits is crucial for sustaining operations and fostering growth. Given their emphasis on economic efficiency, SMEs can impact the broader supply chain's integrity if they either prioritize or neglect security measures (Verbano and Venturini, 2013). The alarming statistic that 99% of the 347,000 manufacturers in the USA are small and medium-sized, with 50% lacking fundamental cyber technology, raises concerns for national security, especially since most cyberattacks targeted these businesses in 2014 (DoD, 2018). Their limited financial and technical resources make them susceptible targets for cyber risks. Large-scale defense industry companies commonly engage in contracting and subcontracting. For instance, when Boeing produced the 747 aircraft in 2012, it comprised 6 million sub-parts sourced from over 550 suppliers in 30 countries (Boeing, 2013). Airbus, with 1,676 publicly disclosed suppliers, has over 12,000 "second-tier and below" suppliers, and General Motors has 856 "first-tier" suppliers along with more than 18,000 "second-tier and below" suppliers. This intricate, multi-layered structure poses challenges in securing the supply chain, particularly as third- and fourth-tier suppliers tend to be smaller and more specialized. These suppliers might also outsource components or operations, introducing "fourth-party" suppliers, further complicating management (Sen, 2019). The complexity of the supply chain with its sub-layers makes tracking sources of risks and vulnerabilities increasingly challenging (Norris et al., 2020: 73). Regardless of how effectively main contractors safeguard their data, the sensitivity remains if adequate precautions are not taken for subcontractors. For example, the 2020 cyber attack on Visser Precision, a subcontractor for major companies such as Lockheed Martin, General Dynamics, Boeing, and SpaceX, exposed extensive data, leading to virtual blackmail threats of further disclosures (Gresik, 2020).

3. DEFENSE SUPPLY CHAIN RISK MANAGEMENT STRATEGIES

The supply chain encompasses all activities performed by manufacturers and distributors to generate value, including purchasing, production, and distribution. Supply chain risk management involves identifying and managing risks across the supply chain to enhance overall resilience and responsiveness

through a coordinated effort among supply chain members (Norris et al., 2020: 69). The U.S. Department of Defense defines Supply Chain Risk Management as "a systematic process used to manage supply chain risk by identifying vulnerabilities, threats, and risks throughout the supply chain and developing mitigation strategies to address these threats posed by the supplier, product, and its subcomponents, or the supply chain" (DoD, 2012).

Supply chain management strategy is how a company enhances its performance through competitive priorities such as quality, flexibility, innovation, speed, time, and reliability (Chen and Paulraj, 2004). These priorities usually encompass cost, quality, flexibility, innovation, speed, time, and reliability, with the overarching goal of ensuring a competitive advantage (Schnetzler et al., 2007). While various supply chain strategies have been suggested by researchers, approaches other than "lean and agile" and "efficient and responsive," which are often used interchangeably, are considered overly simplistic (Basnet and Seuring, 2016).

Lean strategy: Aims to eliminate all waste, including time (Naylor et al., 1999).

Agile strategy: Focuses on responding quickly to unpredictable changes in demand or supply (Christopher and Peck, 2004).

Efficient strategy: Concentrates on reducing unit costs by minimizing long production times and high setup costs (Randall et al., 2003).

Companies that prioritize low cost, high quality, and/or short delivery time typically opt for a lean strategy, whereas those emphasizing flexibility may find an agile strategy more suitable (Qi et al., 2017). Supply chain strategy acts as a response to external and unforeseen factors like demand variability/uncertainty, product variety, desired customer delivery time, and supply uncertainty/risk (Basnet and Seuring, 2016). The primary variables guiding the choice of a supply chain strategy are risks and uncertainties. Supply chain risk management strategies can be broadly classified into two categories: redundancy and flexibility. The redundancy approach involves keeping some resources in reserve to be utilized in case of a disruption. Common examples of this approach include maintaining strategic inventory, having safety stock, engaging multiple suppliers, and adding capacity (Sheffi and Rice, 2005).

In contrast, the resilience strategy is founded on the principle of developing organizational and inter-organizational capabilities to swiftly detect and respond to threats to supply continuity (Zsidisin and Wagner, 2010: 3). Strategies that

promote collaboration, integration, information sharing (communication), and increased responsiveness are examples of flexible risk management strategies. Looking at it from the defense industry perspective, distinct strategies may be required to manage supply chain risks. The primary reason for this is the prominence of national security and sustainability concerns in defense supply chains. Strategies prioritizing national security and the sustainability of the production line are essential. Examples of risk management strategies include risk and return-sharing partnerships, the adoption of new digital technologies, vertical integration, monitoring subcontractors' security systems (stipulating this in contract negotiations), shared supply chains on common platforms, creating an alternative supplier network through multi-sourcing, and involving local players in the global supply network (E&Y, 2018). Strategy choices can significantly enhance the likelihood of achieving corporate goals if they are grounded in the institutionally implemented risk management process. Studies examining the impact of Enterprise Risk Management on corporate performance support this approach (Florio and Leoni, 2016: 56).

Managing defense supply chain risks is of vital importance for national security, and failure to manage these risks may lead to irreparable consequences. Therefore, the initial step for the defense supply chain involves risk analysis. Risk analysis assists organizations in identifying potential vulnerabilities and assessing how these vulnerabilities may impact the organization and its systems (Sobb et al., 2020: 1863). To identify vulnerabilities and high-risk areas in the supply chain, data must first be collected. Three fundamental factors should always be considered when collecting data: 1. the relative importance of the product in terms of national security; 2. the health of the sectors and organizations producing the product (including whether the material is produced at the required capacity/rate and whether the supplier is the sole/primary source); and 3. where the product is manufactured—whether domestically, in an allied or friendly country abroad, or in a competitor or potential competitor country abroad. This approach allows decision-makers to take more informed steps when making decisions regarding the supply chain (Clark, 2021). After collecting the data, the sensitivity or criticality of the products and their impact on the supply chain should be examined, and the probability of the risk occurring should be evaluated. Methods for identifying risks include brainstorming, interviews,

workshops, supply chain mapping (Gardner and Cooper, 2003), the Delphi Method (Linstone and Turoff, 2002), Fault or Event Tree Analysis (Ziegenbein and Nienhaus, 2004), and the Nominal Group Technique (Zsidisin et al., 2000). Vulnerabilities are features likely to disrupt a specific product or service, evaluated at both macro and micro levels. At the micro level, the financial performance of the enterprise and its process structure within the public and private sectors are assessed. At the macro level, the evaluation extends to the market, considering factors like the number of companies in a sector and the level of dependence on foreign suppliers. Criticality pertains to features that make changing a product or service challenging and is assessed concerning the difficulty of recovering from a disruption in a specific sector. Six measures determine criticality: Facility and equipment requirements, Skilled workforce requirements, Defense design requirements, Defense uniqueness, Regeneration time, and Availability of alternatives (DoD, 2014). When assessing risks based on impact and probability, an essential factor is the degree of importance for national security. While many defense sector products are vital for national security, some hold more significance than others. For instance, the spare part of the F-35 aircraft is more critical than a soldier's boot in terms of national security (Clark, 2021).

Following risk assessments, results such as high probability-high impact, high probability-low impact, low probability-high impact, or low probability-low impact are obtained. Some authors (Steele and Court, 1996) assign a relative weight to the probability of occurrence, while others (Ziegenbein and Nienhaus, 2004) categorize the probability as unlikely, possible, probable, or very likely. The impact of a risk is influenced by its scale, scope, duration, recovery time, and total cost. Total impact can be ranked as low or high (Steele and Court, 1996) or low, moderate, significant, or fatal (Ziegenbein and Nienhaus, 2004). Risks are prioritized based on their importance to the organization to eliminate and reduce risks, focusing resources on the most critical ones. The main determinant of how risks are managed is the institution's risk appetite. Institutions with high risk appetite may choose not to manage low-probability risks, even if their impact is high, whereas risk-averse institutions may manage all risks. For example, they might maintain excessive stock to manage disruptions in the supply chain. The redundancy strategy's primary motivation is risk aversion and ensuring supply chain reliability. The global proliferation of supply chains

increases vulnerability to high severity/low probability risks (Sheffi and Rice, 2005). The ongoing Covid-19 epidemic, initially considered a low-probability, high-impact risk, significantly affected all supply chains, including those in the defense industry. Businesses employing Just-in-Time (JIT) production or relying on single resources for high efficiency are more susceptible to high-impact, low-probability risks and experience greater impact when such risks occur (Black and Ray, 2011: 17). Therefore, strategies focused on maintaining redundancy rather than flexibility for managing high-probability, low-impact risks can be more effective (Chang et al., 2015: 648). However, redundancy strategies are closely tied to available resources. As an example, the Defense Logistics Agency (DLA) in the US has maintained a stock of $1.152 billion in 37 types of elements called "Rare Elements" since 1989 to minimize the impact of unforeseen risks in defense supply chains (Dyatkin, 2020). High probability and low impact risks are those encountered regularly in daily activities but have minimal impact. Such risks are relatively predictable, and resilience strategies, supported by collaboration and information exchange among supply chain members, can effectively manage them (Wieland and Wallenburg, 2013). High impact, high probability risks represent frequent occurrences with severe impacts on ongoing business performance, like the loss or failure of a key supplier, labor unrest, unexpected product quality issues, and product recalls. Organizations should prioritize managing and preventing such high severity/high probability risks due to their significant consequences. It may be necessary to employ both redundancy and flexibility strategies concurrently in managing these risks. While the redundancy strategy aims to mitigate short-term, potentially devastating consequences by buying time to address these risks, the communication and collaboration associated with the resilience strategy reduce the likelihood of ongoing significant damage by improving the bounce-back capabilities of supply chain participants (Chang et al., 2015: 649).

When allocating resources after conducting risk analysis, defense industry companies should evaluate the effects and possibilities of risks, prioritize them, and determine strategies appropriate to the type of risk. While flexibility is necessary to manage some risks, redundancy strategies are essential for others. It is nearly impossible or extremely expensive and time-consuming to eliminate all risks in the supply chain. Instead of complete elimination, the impact of risks can be reduced by implementing countermeasures or

mitigation measures throughout the life cycle of the part or system. There are four basic ways to respond to identified risks: using protective measures (countermeasures and mitigations) to reduce the likelihood or consequence of a threat exploiting a vulnerability, transferring some or all of the risk mitigation responsibility to another organization and/or life cycle stage, making a conscious decision to continue the activity (or acquisition) despite possible consequences, or eliminating the possibility of a threat, susceptibility to a vulnerability, or the impact of exploitation by not continuing the activity or acquisition (Ferry and Poindexter, 2016: 21). If the probability, consequence, or duration of a risk cannot be reduced, the institution must determine forward-looking operational, risk-sharing, or transfer measures to mitigate it (Ziegenbein and Nienhaus, 2004).

Responding to risk can range from doing nothing to redesigning a system to avoid using a component that lacks acceptable risk mitigation options. Risk mitigation demands significant effort and has a substantial impact on cost and time. For instance, evaluating the security and privacy practices of all third parties and tracking the points where they share data are risk management techniques requiring substantial effort (Ponemon and Opus, 2018). However, significant costs may be necessary to implement these measures. Choosing an option that requires less effort might save upfront costs but often results in higher costs later in the system's life cycle. Vulnerabilities detected early in a system's design can often be significantly reduced or eliminated at relatively low cost with simple design changes or purchasing restrictions (Ferry and Poindexter, 2016: 22). Emerging technologies and new applications can also be employed to manage supply chain risks. For example, although current applications of Blockchain for supply chain management are limited in scale, this technology can securely store and organize data, making it easily updatable and reducing costs, addressing the obsolescence problem. However, a blockchain application in defense would likely require a centralized network of computers, rather than the decentralized network of servers used in the case of Bitcoin. Similarly, Artificial Intelligence (AI) applications can also be utilized. AI can be employed to detect supply chain weaknesses by scanning data or processing country-of-origin data for components to determine whether these components meet local supply requirements (Clark, 2021).

4. CONCLUSION

Managing supply chain risks in alignment with physical, human, and organizational resources, along with industry dynamics, is a crucial capability for corporate competition and sustainability. Institutions' inability to effectively respond to supply chain risks can lead to disruptions in their operations, a concern highlighted during the supply chain challenges observed in the Covid-19 pandemic. The strength of supply chains relies on the resilience of each link, emphasizing that chain size increases sensitivity. Unforeseen risks within the supply chain can render it vulnerable. Research indicates that supply chain risks may vary across sectors. Therefore, the risk management process for the defense industry supply chain, a fundamental pillar of national security, must cater to the unique needs of the sector. However, defense industry supply chains have received less research attention compared to other supply chains due to product complexity, data accessibility challenges, and intricate economic networks.

The defense industry supply chain, built on long-term collaborations, is among the sectors experiencing rapid changes in the ecosystem. Effectively managing supply risk by adapting to emerging trends like digital advancement and sustainability will be pivotal for a sustainable future in the defense industry. While greater globalization in defense supply chains can offer cost benefits, it also introduces complexity, especially when businesses within the chain have separate sub-chains, complicating relationship management. A supply chain weakened by the Covid-19 pandemic is recognized as a threat to US national security, as highlighted in a supply risks report prepared for presentation to the US Senate. In summary, risks related to supply chains in the defense industry encompass supplier-related risks, risks arising from globalization and foreign dependency, sector-specific risks, and cyber security risks.

Sole-source procurement is an approach that, in many defense industry supply chains, is a necessity rather than a conscious choice, representing one of the most common risks in the defense sector. The widespread adoption of single sourcing in various defense industry areas makes the sector susceptible to global and local supply shortages, ultimately reducing readiness. Another supplier-related risk involves the use of unreliable, imitation, or poor-quality products from subcontractors, posing a significant threat to life in defense systems.

Similar to other sectors, the defense industry relies on numerous

raw materials, intermediate products, and goods, with the added complexity that these items can change hands between different countries. However, political fluctuations can disproportionately impact defense supply chains, leading to severe consequences. The Covid-19 pandemic vividly demonstrated the risks associated with foreign dependency in the defense sector, unveiling vulnerabilities during disruptions. Defense supply chains must meet availability and readiness requirements in times of peace and shift to sustainability requirements during combat. Another challenge for the defense sector is the substantial investment costs imposed on businesses operating in this field due to the stringent safety and security systems, quality assurance standards, and heavily regulated processes required for defense systems.

The sectors struggle to attract sufficient investment often results in continued reliance on traditional suppliers, limiting innovation opportunities. Today, cybersecurity threats, encompassing counterfeit products, unauthorized production, tampering, theft, malware and hardware insertion, as well as subpar production and development practices in the cyber supply chain, have emerged as the foremost risks in defense supply chains. The high success rate of cyber attacks, coupled with the significant damage they cause, underscores the criticality of addressing this issue. Particularly, small and medium-sized enterprises (SMEs) in the sector, lacking the resources for robust cybersecurity measures, become prime targets for cyber hackers.

Managing supply risks requires an effective and comprehensive corporate risk management process. The supply chain strategy acts as a response to external and unexpected factors such as demand variability/uncertainty, product variety, desired customer lead time, and supply uncertainty/risk. While lean and agile strategies, or redundancy and flexibility strategies, are commonly used in supply chain management, the main determinants for choosing a strategy are the risks and uncertainties that guide the selection of the supply chain strategy.

What sets defense supply chains apart is the heightened focus on national security and sustainability concerns. Strategies prioritizing national security and production line sustainability become imperative. However, these strategic choices can only enhance the likelihood of achieving corporate goals if they are rooted in a robust corporate risk management process. The initial step for defense supply chains involves risk analysis. The examination of product sensitivity or criticality within the chain, along with its

impact on the supply chain, should be closely assessed, and the probability of the risk occurring must be evaluated.

The impact and probability resulting from risk assessments determine the significance of the risk and become the primary factor influencing decisions on managing the institution within the established risk appetite or allocating resources. The expanding scope of global supply chains exposes companies to increasing vulnerability to high severity/low probability risks. In the management of high probability and low impact risks, strategies emphasizing redundancy take precedence, whereas flexibility strategies prove more effective for high probability and low impact risks—risks encountered in daily activities that lack a significant impact.

High probability and high impact risks necessitate comprehensive management by the institution and may require the simultaneous use of both flexibility and redundancy strategies. The notion of eliminating all risks in the supply chain is practically unattainable and can be excessively costly and time-consuming. Instead of total elimination, reducing the impact of risks through countermeasures or mitigation measures throughout the part or system's life cycle offers a more practical approach.

Responding to risk encompasses a broad spectrum of activities, ranging from taking no action to utilizing all available resources. This involves a trade-off, as significant costs may need to be incurred to eliminate substantial risks. Conducting risk analyses from the outset, especially during the design or installation phase of the supply chain, plays a crucial role in averting larger risks that might surface over time. Therefore, risk management in defense supply chains should consistently be an integral part of the process.

REFERENCES

[1] Alicke, K., Davies, A., Leopoldseder, M. and Niemeyer, A., (2017), Blockchain Technology for Supply Chains—A Must or a Maybe?" McKinsey & Company, September 12, retrieved in 25.10.2021 from: https://www.mckinsey.com/business-functions/operations/our-insights/blockchain-technology-for-supply-chainsa-must-or-a-maybe

[2] Barney, J., (1991), "Firm Resources and Sustained Competitive Advantage", Journal of Management, 17 (1): pp. 99–120.

[3] Basnet, C. and Seuring, S. (2016), "Demand-oriented Supply Chain Strategies – a Review of the Literature", Operations and Supply Chain Management: An International Journal, Vol. 9 No. 2, ss 73-89, doi: 10.31387/oscm0240162.

[4] Beske, P., Land, A. and Seuring, S., (2014), "Sustainable Supply Chain Management Practices and Dynamic Capabilities in the Food Industry: A Critical Analysis of the Literature. International" Journal of Production Economics, 152: pp.131–143.

[5] Bluevoyant, (2021), "Defense Industry Supply Chain & Security 2021", Bluevoyant Review,
[6] Boeing, (2013), "Boeing Celebrates Delivery of 50th 747-8", retrieved in 16.11.2021 from https://boeing.mediaroom.com/2013-05-29-Boeing-Celebrates-Delivery-of-50th-747-8
[7] Bradsher, K., (2010), "Amid Tension, China Blocks Vital Exports to Japan", The New York Times, September 22, retrieved in 25.10.2021 from https://www.nytimes.com/2010/09/23/business/global/23rare.html
[8] Cabral, I., Grilo, A. and Cruz-Machado, V., (2012) "A Decision-Making Model for Lean, Agile, Resilient and Green Supply Chain Management", International Journal of Production Research Vol. 50 No. 17, pp. 4830-4845.
[9] Chang, W., Ellinger, A.E., Blackhurst, J., (2015), "A Contextual Approach to Supply Chain Risk Mitigation", The International Journal of Logistics Management, Vol. 26 No. 3, pp. 642-656. https://doi.org/10.1108/IJLM-02-2014-0026.
[10] Chen, I.J. and Paulraj, A., (2004), "Towards a Theory of Supply Chain Management: the Constructs and Measurements", Journal of Operations Management, Vol. 22 No. 2, pp.119-150.
[11] Chipeta, C. (2021) "What Is Fourth Party Risk?," UpGuard, November 19, 2021, retrieved in 26.10.2021 from https://www.upguard.com/blog/
[12] Christopher, M. And Peck, H., (2004) "Building the resilient supply chain", The International Journal of Logistics Management, Vol. 15 No. 2, pp. 1-14.
[13] Clark, M., (2021), "Understanding and Protecting Vital U.S. Defense Supply Chains. Backgrounder No. 3598" | April 1, Center For National Defense.
[14] Darby, J.L., Ketchen, D.J Jr., Williams, B.D. and Tokar, T., (2020), "The Implications of Firm-Specific Policy Risk, Policy Uncertainty, and Industry Factors for Inventory: A Resource Dependence Perspective". Journal of Supply Chain Management XX (XX): 1–22.
[15] Davis, D.B., (2019), "ISTR 2019: Cyber Criminals Ramp Up Attacks on Trusted Software and Supply Chains". Symantec Expertise Block, retrieved in 11.10.2021 from https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/istr-2019-cyber-criminals-ramp-attacks-trusted-software-and-supply-chains
[16] DoD, (2012), Instruction (DoDI) 5200.44, Supply Chain Risk Management (SCRM),
[17] DoD, (2016), "U.S. Department of Defense, Annual Industrial Capabilities" Report to Congress for 2014, September p. 8, retrieved in 25.10.2021 from: https://www.businessdefense.gov/Portals/51/Documents/Resources/2014%20AIC%20RTC%2010-03-16%20-%20Public%20Unclassified.pdf?ver=2017-04-18-072624-770
[18] DoD, (2018), Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States, Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806.
[19] Dowdall, P., (2004), "Chains, Networks and Shifting Paradigms: The UK Defence Industry Supply System". Def. Peace Econ15, pp.535–550.
[20 Dyatkin, B., (2020), "COVID-19 Pandemic Highlights Need for US Policies that Increase Supply Chain Resilience". MRS Bulletin, Volume 45, October.
[21] Ekström, T., Hilletofth, P. and Skoglund, P., (2020), "Differentiation Strategies for Defence Supply Chain Design", Journal of Defense Analytics and Logistics, Vol. 4 No. 2, pp. 183-202.https://doi.org/10.1108/JDAL-06-2020-0011.

[22] E&Y, (2017), "Top 10 Risks in Aerospace and Defence (A&D)" retrieved in 25.10.2021 from https://www.ey.com/en_gr/aerospace-defense/the-top-10-risks-in-aerospace-and-defense
[23] E&Y, (2018), "A&D Edge Supply Chain Management in Aerospace and Defense" February 2018.
[24] E&Y, (2021), "How to reshape aerospace and defence supply chains for resilience" retrieved in 20.10.2021 from https://www.ey.com/en_uk/aerospace-defense/how-to-reshape-aerospace-and-defence-supply-chains-for-resilience
[25] Ferry H., and Poindexter, (2016), "Suply Chain Risk Management, An Introduction to Creadible Threat", Defense AT&L: July-August 2016
[26] Florio, C. and Leon, G., (2017), "Enterprise Risk Management and Firm Performance: The Italian Case", The British Accounting Review, Volume 49, Issue 1, pp. 56-74.
[27] Friesen, G., (2021), "No End In Sight For The COVID-Led Global Supply Chain Disruption", Forbes, 2021, retrieved in 10.10.2021, from https://www.forbes.com/sites/garthfriesen/2021/09/03/no-end-in-sight-for-the-covid-led-global-supply-chain-disruption/?sh=37fef8053491
[28] GAO, (2020), "F-35 Joint Strike Fighter. Actions Needed to Address Manufacturing and Modernization Risks". United States Government Accountability Office Report to Congressional Committees. GAO-20-339.
[29] Gardner, J.T. and Cooper, M.C., (2003), "Strategic Supply Chain Mapping Approaches", Journal of Business Logistics, Vol. 24, No. 2, pp. 37–64.
[30] Garvey, M.D., Carnovale, S. and Yeniyurt, S., (2015), "An Analytical Framework for Supply Network Risk Propagation: A Bayesian Network Approach". European Journal of Operational Research 243:618–27.
[31] Gellweiler, C. (2018), "Cohesion of RBV and Industry View for Competitive Positioning". Strategic Management 23 (2): 3–12.
[32] Gill, C. and Pollard, J.,(2020), "China Threatens Rare Earth Blacklist as Trade War Expands", Asia Times Financial, October 12, retrieved in 25.10.2021 from https://www.asiatimesfinancial.com/china-threatens-rare-earth-blacklist-astrade-war-expands
[33] Gohs, I., (2021), "The Biggest Business Risks in 2021", Visual Capitalist, retrieved in from 10.10.2021 https://www.visualcapitalist.com/the-biggest-business-risks-around-the-world/
[34] Gonzalez, A. and Rodriguez, S. (2021), "Nothing left in the tank: The State of the Pentagon's Supply Chain". Defensenews. retrived in 20.10.2021 from: https://www.defensenews.com/opinion/commentary/2021/06/28/nothing-left-in-the-tank-the-state-of-the-pentagons-supply-chain/
[35] Gould, J., (2020), "COVID Closed Mexican Factories That Supply U.S. Defense Industry. The Pentagon Wants Them Opened," Defense News, April 21, retrieved in 25.10.2021, from: https://www.defensenews.com/2020/04/21/covid-closed-mexican-factories-that-supply-us-defense-industry-the-pentagon-wants-them-opened/
[36] Gresik, D. (2020), "A Hacker Group Says it has Major Defense Companies' Data". Fifth Domein, 02 Mart 2020, retrieved in 05.11.2021 from https://www.fifthdomain.com/2020/03/02/a-hacker-group-says-it-has-major-defense-companies-data/
[37] Gunasekaran, A., Papadopoulos, T. et al: (2017), "Big Data and Predictive Analytics for Supply Chain and Organizational Performance". Journal of Business Research 70: 308–317.

[38] Hachicha, W. and Elmsalmi, M. (2014) "An Integrated Approach Based-Structural Modeling For Risk Prioritization in Supply Network Management". Journal of Risk Research 17: 1301–24.
[39] HASC, (2021) Report Of The Defense Critical Supply Chain Task Force. House Armed Services Committee July 22, 2021.
[40] Haren, P. and Simchi-Levi, D., (2020), "How coronavirus could impact the global supply chain by midMarch", Harvard Business Review, Vol. 28., retrieved in 10.10.2021 from: https://hbr.org/2020/02/how-coronavirus-could-impact-the-global-supply-chain-by-mid-march
[41] Humphries, M., (2015), "China's Mineral Industry and U.S. Access to Strategic and Critical Minerals" Issues for Congress.
[42] Inoue, Y., (2010) "China Lifts Rare Earth Export Ban to Japan: Trader", Reuters, September 29, https://www.reuters.com/article/us-japan-china-export-idUSTRE68S0BT20100929.
[43] James, A.D. (2009), "Reevaluating the Role of Military Research in Innovation Systems: Introduction to the Symposium." J. Technol. Transfer, 34, 449–454.
[44] Kluth, M., (2017), "European Defence Industry Consolidation and Domestic Procurement Bias". Def. Secur. Anal., 33, 158–173.
[45] Larson, D., (2018), "Global Survey Reveals Supply Chain as a Rising and Critical New Threat Vector", CrowdStrike Blog, retrieved in 12.10.2021 from https://www.crowdstrike.com/blog/global-survey-reveals-supply-chain-as-a-rising-and-critical-new-threat-vector/
[46] Li, S., Ragu-Nathan, B., Ragu-Nathan, T.S. and Rao, S.S., (2006), "The Impact of Supply Chain Management Practices on Competitive Advantage and Organizational Performance", Omega, Vol. 34 No. 2, pp. 107-124.
[47] Linstone, H.A. and Turoff, M., (2002), The Delphi Method: Techniques and Applications, http://www.is.njit.edu/pubs/delphibook/
[48] Lye, H., (2020), "Expect shrinking budgets and change of military focus: Globsec on Covid-19". Army-technology.com. retrieved in 25.10.2021 from, https://www.army-technology.com/features/expect-shrinking-budgetsand-change-of-military-focus-globsec-on-covid-19/
[49] Menz, R., (2018) "Can We Defend The Defense Supply Chain? Lessons Learned From Industry Leaders In Supply Chain Management". Naval Postgraduate School.Thesis Research.
[50] NIST, (2020), "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry". NISTIR 8276, retrieved in 11.10.2021 from: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf
[51] Norris, W., Rodgers, J.B., Blazek, C., Hewage, T. and Kobza, B., (2020), A Market-Oriented Approach to Supply Chain Security. Security Challenges, Vol. 16, No. 4, Geo-Economics in the Indo-Pacific, pp. 65-81
[52] Ponemon, L., (2018), "Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks", Businesswire November 15, retrieved in 11.10.2021 from https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Results-2018-Third-Party
[53] Porter, M., (1981), "The Contributions of Industrial Organization to Strategic Management". Academy of Management Review 6 (4): pp.609–620.
[54] Pyman, M., Wilson, R. and Scott, D., (2009), "The Extent Of Single-sourcing In Defence Procurement And Its Relevance As

A Corruption Risk: A First Look", Defence and Peace Economics, Vol. 20(3), June, 215-232
[55] Qi, Y., Huo, B., (2017), "The impact of Operations and Supply Chain Strategies on Integration and Performance", International Journal of Production Economics, Vol. 185, pp. 162-174.
[56] Rajagopal, R. And Ravi, V., (2015), "Modeling Enablers of Supply Chain Risk Mitigation in Electronic Supply Chains: a Grey-DEMATEL Approach". Computers & Industrial Engineering 87: 126–139. doi:10.1016/j.cie.2015.04.028.
[57] RAND, (2021), "Productivity challenges and UK defence supply chains". RAND Europe Publications. Retrieved in 25.10.2021 from: https://www.rand.org/randeurope/research/projects/challenges-and-barriers-to-uk-defence-supply-chains.html
[58] Randall, T.R., Morgan, R.M., and Morton, A.R., (2003), "Efficient Versus Responsive Supply Chain Choice: an Empirical Examination of Influential Factors", Journal of Product Innovation Management, Vol. 20 No. 6, pp.430-443.
[59] Ray, S. and Black, T., (2011), "Downside of just-in-time inventory", Businessweek, 24 March, pp.17-18.
[60] Samvedi, A., Jain V. And Chan F. T.S., (2013), "Quantifying Risks in a Supply Chain Through Integration of Fuzzy AHP and Fuzzy TOPSIS". Int J Prod Res 51(8): 2433–2442. https://doi.org/10.1080/00207543.2012.741330.
[61] Satariano, A. (2013) "The IPhone's Secret Flights from China to Your Local Apple Store," Bloomberg, September 11, https://www.bloomberg.com/news/2013-09-11/the-iphone-s-secretflights-from-china-to-your-local-apple-store.html.
[62] Schnetzler, M.J., Sennheiser, A. and Schonsleben, P., (2007), "A Decomposition-Based Approach for the Development of a Supply Chain Strategy", International Journal of Production Economics, Vol. 105 No. 1, pp. 21-42.
[63] Sheffi, Y. and Rice J.B. Jr., (2005), "A Supply Chain View of the Resilient Enterprise", MIT Sloan Management Review, Vol. 47 No. 1, pp. 41-48.
[64] Sisk, R., (2020), "US to Keep Buying F-35 Parts From Turkey, Despite Purchase Ban". Military.com, retrieved in 25.10.2021 from: https://www.military.com/daily-news/2020/10/01/us-keep-buying-f-35-parts-turkey-despite-purchase-ban.html
[65] Smyth, J., (2020), "Industry Needs a Rare Earths Supply Chain Outside China", Financial Times, July 28, 2020, retrieved in 25.10.2021 from https://www.ft.com/content/fc368da6-1c86-454b-91ed-cb2727507661
[66] Sofyalıoğlu, Ç. and Kartal, B., (2012), "The Selection of Global Supply Chain Risk Management Strategies by Using Fuzzy Analytical Hierarchy Process—A Case from Turkey". Procedia—Social and Behavioral Sciences 58:1448–57.
[67] Sobb, T., Turnbull, B. and Moustafa, N., (2020), "Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions", Electronics.; 9(11): 1864. https://doi.org/10.3390/electronics9111864
[68] Son, J.Y. and Orchard, R.K.,(2013), "Effectiveness of policies for mitigating supply disruptions", International Journal of Physical Distribution & Logistics Management, Vol. 43 No. 8, pp. 684-706.
[69] Srivastava, M. and Rogers, H., (2021), "Managing Global Supply Chain Risks: Effects of the Industry Sector". International Journal of Logistics Research and Applications, 1–24. doi:10.1080/13675567.2021.1873925.
[70] Steele, P.T. and Court, B.H., (1996), Profitable Purchasing Strategies: A Manager's Guide for Improving Organizational Competitiveness Through the Skills of Purchasing, London: McGraw-Hill Book Co.

[71] Stock, J.R. and Boyer, S.L., (2009) "Developing a consensus definition of supply chain management: a qualitative study", International Journal of Physical Distribution and Logistics Management, Vol. 39 No. 8, pp. 690-711.
[72] Tse, Y.K., Matthews, R. L. (2016), "Unlocking Supply Chain Disruption Risk Within the Thai Beverage Industry". Industrial Management & Data Systems 116 (1): 21–42
[73] Vavra, S. and Stark, T., (2020), "How the Russian Hacking Group Cozy Bear, Suspected in the SolarWinds breach, plays the long game, Syberscoop, retrieved in 21.10.2021 from: https://www.cyberscoop.com/cozy-bear-apt29-solarwinds-russia-persistent/
[74] Verbano, C. and Venturini, K., (2013), "Managing Risks in SMEs: A Literature Review and Research Agenda", Journal of Technology Management & Innovation 8, no. 3: 33–34, https://doi.org/10.4067/S0718-27242013000400017.
[75] Watson, J., (2015), "Essays On Deceptive Counterfeits In Supply Chains: A Behavorial Perspective". All Dissertations, https://tigerprints.clemson.edu/all_dissertations/1589
[76] Wieland, A and Wallenburg, C.M. (2013), "The Influence of Relational Competencies on Supply Chain Resilience: a Relational View", International Journal of Physical Distribution & Logistics Management, Vol. 43 No. 4, pp. 300-320.
[77] Ziegenbein, A. and Nienhaus, J. (2004), "Coping with Supply Chain Risks on Strategic, Tactical, and Operational Level," Proceedings of the Global Project and Manufacturing Management, Symposium, Siegen, pp. 165–180.
[78] Zsidisin, G.A., Panelli, A. and Upton, R., (2000), "Purchasing Organization Involvement in Risk Assessments, Contingency Plans, and Risk Management: An Exploratory Study", Supply Chain Management, Vol. 5, No. 4, pp. 187–198.
[79] Zsidisin, G.A. and Wagner, S.M., (2010), "Do Perceptions Become Reality? the Moderating Role of Supply Chain Resiliency on Disruption Occurrence", Journal of Business Logistics, Vol. 31, No. 2, ss. 1-20.