The Strategic Promise of Digital Twins to Enhance Supply Chain Resilience

Authors: Monica Adami[1], Mateusz Nowak[1], Maarten Toelen[1], Claudio Valle[1], Arno Van der hasselt[1], Annika Weinmann[1]

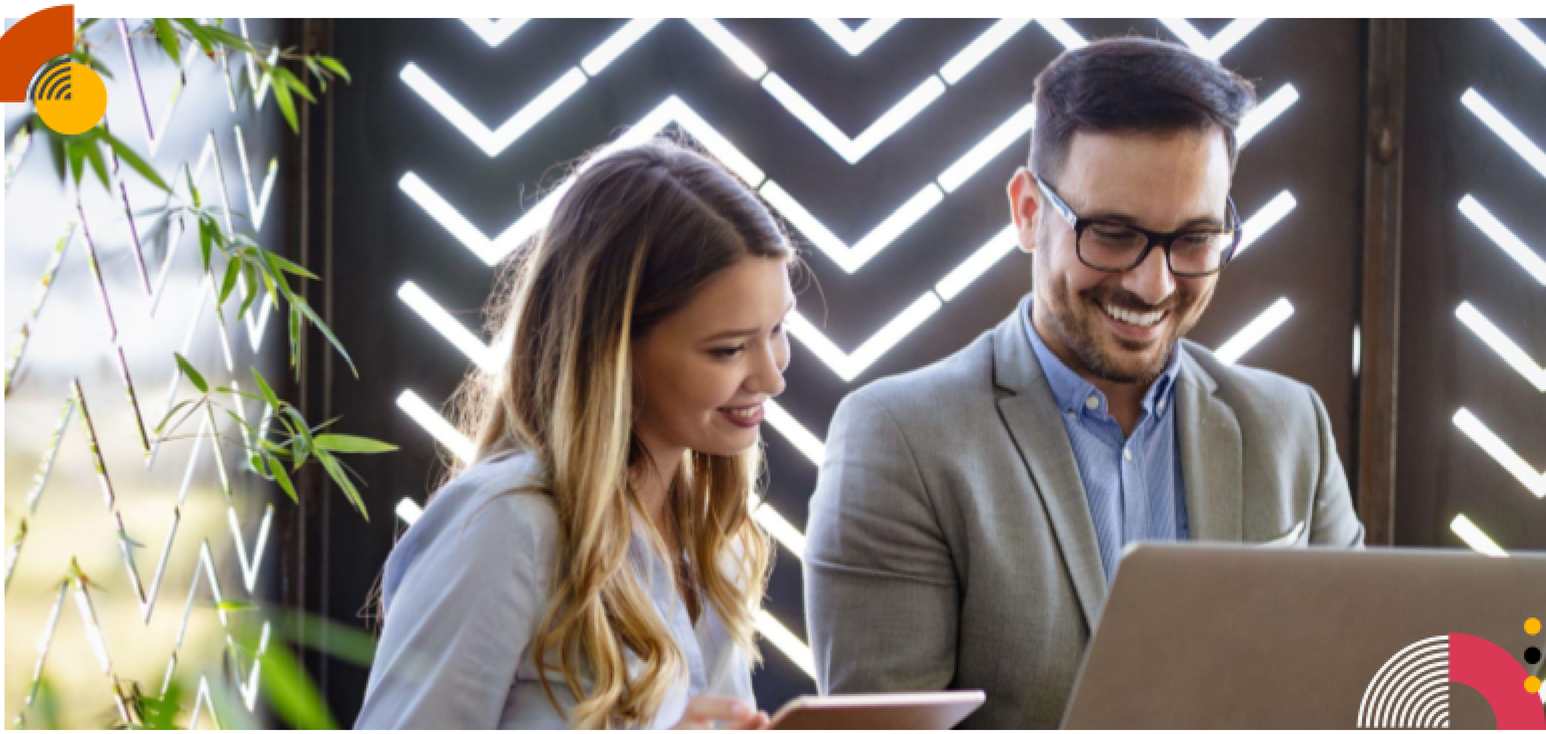
arno.van.der.hasselt@pwc.com, maarten.toelen@pwc.com

Abstract

In recent publications, the European Defence Agency has pointed out the need to make supply chains more resilient, a priority which was further highlighted by Russia's aggression against Ukraine. This paper argues that it is feasible to make (military) supply chains less redundant through the adoption with the help of digital twins as a technological solution. Digital twins offer many advantages, above all real-time monitoring and analysis, which can strategically be combined with innovative crisis simulations and additional supporting technologies, to ensure supply chains survive in adverse and potentially unknown conditions, prevent supply shortages, reduce maintenance costs and time, and enable collaboration with other partners and stakeholders.

Keywords

Digital twins, Supply Chain Resilience, Data interoperability, Dual-use



[1] PricewaterhouseCoopers Enterprise Advisory BV, Belgium

1. Context and Introduction

In June 2018, the EDA's Capability Development Plan (CDP) underwent a significant revision, which resulted in the definition of 11 European capability development priorities, including *enhanced logistic and medical supporting capabilities*. Similarly, the Overarching Strategic Research Agenda (OSRA) defines common R&T priorities in the form of Technology Building Blocks (TBB), amongst which is the *Defence critical technologies supply chain* (TBB45). As illustrated by the ongoing war in Ukraine, military supply chains - and their resilience towards issues like terrain, maintenance costs, availability of materials - have become crucial elements in defence.

It has rightfully become an EDA priority to make military supply chains more resilient. Building further upon this priority, this paper aims to explore a possible way forward to make military supply chains less redundant. In the context of supply chains, redundancy refers to having back-up systems, processes, or resources in place to ensure that operations can continue in the event of unexpected disruptions, for instance, due to an adversary offensive, natural disasters, geopolitical instability or equipment failures.

Digital twins are a key enabling technology that allows civil and military stakeholders to precisely simulate calamities and develop better and intelligence-driven decision-making in order to mitigate such crisis events. Identifying dependencies, bottlenecks and weaknesses in the provision of critical materials and assets - both primary and subsidiary - can also assist in better preparing resilience plans and strategies at a lower cost. In addition, through the usage of digital twins, civil and military stakeholders can monitor production processes, identify shortages or the absence of supply-chain diversification, in a timely and correct manner. Particularly in a domain such as military logistics, where high fidelity and low fault tolerance are crucial, digital twins have a genuine potential to improve and facilitate military supply chains.

The operationalisation of digital twins in itself is no novelty however, as numerous examples of this innovative technology have already been adopted in (military) aviation. In 2018, the Turkish Aircraft Industries Corporation entered an agreement with Siemens Product Lifecycle Management software to implement a complete digital twin in the company's manufacturing enterprise; in 2020, the US military used digital twin technology to improve planning and efficiency of F-35 fighter jets and Sikorsky UH-60 Black Hawk helicopters, and in 2021 Rolls Royce turned to digital twins to improve jet engine efficiency (Mendi et al. 2022).

While this technology is already present in (military) aviation, there is vast untapped potential for it to be developed and implemented in other fields of the defence sector and scaled-up to the entire military supply chain - from a single (weapon) system to wider and more complex ones. The integration with other innovative technologies and processes such as 'internet of (military) things', blockchain and intelligence swarming combined with growing computing capabilities can make digital twins an operational reality. Digital twins of this kind would prove to be most effective in cases of cross-border supply chains in order to assess/monitor feasibility of collaborations on international projects (e.g. EMBT or European Patrol Corvette) or in cases of crisis (e.g. humanitarian responses involving military operations, or supply of critical equipment/materiel to allies and partners such as Ukraine).

2. Business Case

The military supply chain is a complex and multifaceted ecosystem that involves various interconnected processes such as the acquisition, storage, transportation, and distribution of equipment, supplies and military personnel. As illustrated by recent military operations, resilient and reliable supply chains are vital for societal resilience and in order to ensure operational effectiveness. Be that as it may, the current state of military supply chain management is often characterised by inefficiencies, redundancies and a lack of end-to-end visibility (Sani, Schaefer & Milisavljedvic-Syed 2022).

One of the key characteristics of military supply chains is their redundancy (Katsaliaki, Galetsi & Kumar 2022). By having redundant systems in place, the military can minimise the impact of disruptions on their operations and ensure that goods and services continue to flow. However, redundancy can also lead to inefficiencies and unnecessary complexity if not managed properly. Maintaining excess inventory, for example, can tie up vital resources and increase costs, while having too many redundant suppliers can lead to unnecessary duplication of effort. As such, it is important to carefully balance the need for redundancy with the costs and risks associated with maintaining redundant systems.

2.1. Real-Time Monitoring and Analysis

Digital twins can provide real-time monitoring and analysis of the entire military supply chain, from suppliers to manufacturers, all the way to the end-user. They can thus be used to track inventory levels in real-time, providing a clear picture of which equipment is available and what needs to be replenished, as well as monitor the state of production and predict when maintenance is required. In turn, this would reduce downtime and augment the lifespan of equipment. By doing so, digital twins can help identify potential issues and bottlenecks in the supply chain, allowing for timely intervention to prevent disruptions. For instance, one of the main issues to take into consideration in relation to a military supply chain is the demand fluctuation, i.e., the variance in demand needs and/or budget. Military supply chains are exposed to large fluctuations in orders, going rapidly from orders of a few parts to large quantities, driven by optempo and unforecasted requirements. Taking this into consideration, military supply chains would benefit from the help of digital twins to facilitate end-to-end asset visibility, which ensures that supplies arrive at the right destination and time (Wu et al. 2020). In other words, digital twins can support decision makers by providing them with precise and up-to-date information on the location and conditions of critical military supplies (food, fuel, weapons, equipment, and spare parts) and promptly react to meet operational needs.

Outside of the European Union, one can identify numerous examples of digital twins being used to improve inventory management, repair and maintain military equipment, with the overall objective to optimise military operations. For example, the U.S. Army has developed a digital twin of its supply chain, called the Global Combat Support System-Army (GCSS-Army). GCSS-Army is a web-based logistics information system that provides real-time visibility into inventory levels, transportation status, and delivery times. It has been field-tested in various military operations, such as those in Iraq and Afghanistan, where it helped to reduce redundancies in the vast operational supply chain of the U.S armed forces. Another example of a digital twin is the U.S. Navy's Virtual Ship program, which provides real-time data on a Navy ship's systems and operations. This enables the Navy to optimise maintenance and repair schedules, proactively identify potential issues, and reduce downtime.

Whereas digital twins rely on the timely provision of reliable data to render an accurate supply-chain simulation and allow for meaningful scenario simulations, specific (organisational and legal) frameworks should be put in place to ensure that all key stakeholders across the supply chain share responsibility for data quality, especially when data has to be shared cross-border. However, the quality of data in military supply chain management can be variable due to several reasons, such as the complexity of the supply chain, the diversity of data sources and the challenges associated with (classified) data sharing and integration. Indeed, military supply chains involve multiple actors - including manufacturers, suppliers, logistics providers and end users, each with their own data systems and processes - and often operate in challenging environments, such as combat zones or disaster areas, which can affect the quality and availability of data. Legal frameworks can also provide a basis for the resolution of disputes related to data quality issues, as well as establish penalties for failing to meet data quality standards or for breaching agreements related to data management. Lastly, they can also encourage the adoption of best practices and standards for data quality across the supply chain. This can help to ensure that all parties have access to accurate and reliable data, which is essential for effective decision-making and efficient operations in military supply chain management.

2.2. Simulations

In crisis management, critical activities - such as the resilience of a supply-chain - are often subject to regular crisis exercises and testing. This can help military planners prepare for potential disruptions by making informed decisions based on the results of the simulations, developing contingency plans and evaluating their effectiveness. However, those exercises present a lot of drawbacks that reduce their efficiency over a vast military supply-chain: among other things, they are not frequent enough, not adjustable enough, too demanding and they are very expensive. In a fully functioning digital twin, changes in the physical world are directly translated into the virtual replica. The higher the quality of the data provided through sensors, ‘internet of military things’ and IT systems in general, the more accurate is the digital twin, its ability to provide snapshots of the current state and its ability to support simulations.

Through the convergence of crisis management with digital twins, military decision-makers could benefit from game-theoretic decision-making to improve situation assessment, facilitate multi-actor and cross-domain decision making, and increase coordination among various public and private stakeholders.

Besides such macro-level advantages, crisis simulations can also be run to test the resilience of the digital environment - and parts of the supply chain - itself. Simulating a cyberattack and the interruptions in the supply chain caused by it, specific strategies and protocols can be prepared in order to minimise the impact. Having a digital replica and testing different scenarios, can allow for quickly spotting anomalies and detect if reality is matching some of those previously tested scenarios. In this sense, a digital twin has the potential to be used to prevent cyber attacks by learning the behaviour of attackers and increase the security of the entire supply chain against cyber intrusions and malwares (Holmes et al. 2021).

2.3. Key Supporting Technologies and Data Infrastructures

Decentralised approaches to data processing such as ‘edge computing’ are pertinent in order to feed the digital environment with the necessary data flows. Edge computing is not a new concept in the military environment and has been successfully applied e.g. in the air domain, coupled with AI to gain military advantages based on information superiority (Zhou et al. 2019). This is the case of the F-35 which has unique capabilities to create networks among groups of aircrafts by combining information processed by each aircraft into a single stream of situational awareness and threat assessment. The scaling-up of edge computing to an entire supply chain environment allows for unprecedented data-driven strategic decision and long term policy-making. In such an environment, even if one node in the supply chain is disrupted, other nodes can continue to operate and provide critical data.

In combination with edge and decentralised computing, existing initiatives on data spaces can be crucial enablers for the pooling of the necessary data use in the digital twin environment. It is expected that in a few years, the European Commission will have successfully led the launch of common European dataspaces in several domains, including manufacturing and the supply chain or the Single European Sky, which has a clear potential to support military interoperability and coordination.

Overall, the combination of edge computing and data spaces can create a more distributed and resilient supply chain ecosystem, where data can be processed and analysed at the edge, while still being integrated into a centralised platform for overall supply chain management. Decentralisation of data collection and processing can make the digital twin more agile and feasible. By bringing computing power closer to the point of data generation, edge computing can reduce latency and improve the speed of data processing. In addition, such an approach can help in identifying new and mitigating the existing risks associated with data breaches and cyberattacks, which are major concerns in military supply chain management.

Moreover, by enhancing data availability and computing capabilities, progressive integration with advanced visualisation technologies can further support the optimisation of military supply chain processes and help limit redundancies. Mixed reality (MR) or extended reality (XR) applications in factories and military warehouses have the potential to provide a realistic simulation environment that allows users to interact with virtual objects and data in real time. For example, MR/XR applications can be used to simulate the placement of equipment and supplies in a military warehouse, enabling users to test different scenarios and optimise layouts for maximum efficiency. In addition, these applications can be used to simulate assembly lines and logistics operations in factories, allowing users to identify bottlenecks, improve workflows, and optimise resource utilisation (Zhou et al. 2019).

2.4. European Collaboration

Initiatives such as *Sharing of Spare Parts* - aiming to manage spare parts for equipment and weapons systems across nations - have proven successful when it comes to collaboration across Member States in the field of military procurement and maintenance. More recently, the European Commission has adopted a proposal for a Regulation to establish the *European Defence Industry Reinforcement through common Procurement Act* for 2022-2024, which is already being used to jointly procure support for Ukraine. Going one step further, digital twins can be used to share data and collaborate across different military units and organisations (Bécue et al. 2020). This could then improve communication and coordination, resulting in more effective supply chain management. By operationalising digital twins, military organisations can facilitate a shared digital platform that provides real-time visibility into the entire military supply chain. In addition to providing a common operating picture for all stakeholders and this help reduce the duplication of efforts, digital twins - used in this manner - can facilitate data sharing by providing a secure space for sharing sensitive information. With the help of advanced encryption and access controls, digital twins can ensure that only authorised personnel has access to sensitive information, while enabling collaboration and information sharing.

By way of example; digital twins have already been used to improve collaboration and coordination between different teams involved in manufacturing processes. By creating a digital twin of a manufacturing process, designers, engineers, and production managers can work together more effectively to optimise production and reduce costs. By integrating digital twins into military supply chains, it will be possible to create virtual replicas of military logistics and supply chain systems, including transportation networks, warehouses, and distribution centres. As such, military logistics personnel from different units or branches can work together to optimise logistics and supply chain operations. Looking into the future, digital twins can foster collaboration but, in turn, they can be improved by collaboration and coordination at European level. To ensure timely data availability, ad hoc systems should be put in place to allow data sharing in secure and trusted environments. To this end, military supply chain data lakes and defence dataspaces could be jointly developed at European level and become the backbone of digital twins, bringing together industry, governments and military structures.

The European Union can support the development of digital twins in several ways. The EU can provide funding and resources to support research and development of digital twin technologies. This can help to accelerate the development and deployment of digital twin solutions in conflict scenarios. The technical set-up of the digital twins must include clear approaches to data interoperability, which are at the very essence of data sharing, to ensure that they are interoperable and compatible across different industries and sectors. This means reusing existing standards and formats to ensure alignment with other initiatives (e.g. sectoral data spaces). In addition, the EU can invest in education and training programmes to develop the skills and knowledge necessary to design, develop, and operate digital twin solutions. This can help, for instance, to create a skilled workforce that can ensure high cybersecurity requisites for digital twins, which rely on connectivity and data exchange and are, therefore, vulnerable to cyber threats.

3. Cross-Domain (Civ-Mil) Applicability

The relevance of digital twins also resides in their cross-sector nature and applicability. On the cross-military dimension, there are several systems needing the same type of components to be produced or to function. This is the case when it comes to the same types of microchips used to produce artillery targeting/guiding systems of ships, aircrafts and tanks or same type ammunition which could be deployed in different scenarios. An example of the latter is represented by the Aster missile which can be operated by different launching platforms such as the FREMM frigates or the SAMP/T anti-air land system. Having an up-to-date view of production processes, stocks and location of military goods makes it possible to redeploy them as needed across interoperable systems, addressing pressing needs while allowing for the manufacturers to replenish stocks. This could prove particularly useful in conventional military and alliance operations, where large scale pooling of military resources across different countries put inventories and manufacturers under pressure. The emergency exposed relatively late widespread issues in production and supply chain capabilities which could have been preemptively detected through accurate and data-driven simulations.

In addition to the purely military dimension, a digital twin designed to support military supply chains has to also gather data from the manufacturing industry, from logistical services, and from critical service providers (e.g. energy). For instance, European manufacturers in many strategic fields are dependent on supplies of critical raw materials and intermediate goods for their production. These include for instance lithium, semiconductors and microchips which are crucial not only for the military systems, but also for the regular production of vehicles or electronic medical equipment, used in everyday life and crucial in times of crisis. This is also in line with latest EU policies such as the *Critical Raw Materials Act* which clearly states the need to ensure a secure and sustainable supply of raw materials for Europe's industry, which is at the core of the green transition, and in general to long-term European competitiveness and autonomy at world's level.

The preservation of minimum levels of strategic production capabilities is required to ensure that the supply chain of critical goods is constantly monitored and diversified. A digital twin would enable it to run simulations on supply shortages and cuts to key manufacturers and critical services, and preventively act to prepare contingency plans for uninterrupted supply chains.

Energy (both in terms of energy grids and fuels) is another case of critical supply chain which should be monitored for ensuring that the operativity of military installations and systems would not be altered in case of natural or man-caused adverse events. However, there are additional critical infrastructures which must be kept operational including not only hospital or government buildings, but also production lines and delivery of primary goods, from ammunition factories to food processing sites. Digital twins related to energy supply already exist and are used to inform decision making and support energy shortages responses. Pooling data on energy supplies into a broader security dimension, would allow them to extend their scope and support both military and civilian preparedness and resilience.

It is therefore clear that the infrastructure needed to develop digital twins can also be kept in use in times of peace and be deployed to address and prevent issues which are specifically related to the military dimension.

4. Conclusions and Recommendations

When considering operational lessons learnt from the Russian aggression against Ukraine, General Robert Brieger, Chairman of the EU Military Committee, highlighted that “logistics, often considered secondary compared to operational aspects, have once more demonstrated their crucial impact on warfare: footage of tanks out of fuel, kilometres-long convoys stalled on the street sides and soldiers hunting for food will fill history books with powerful images” (European Defence Agency 2022). In this regard, the importance of resilient and efficient supply chains in a military environment cannot be overstated.

This paper proposes to use digital twins to make supply chains more resilient and efficient by reducing their redundancy, which is a characteristic inherent to all supply chains, military ones included. In particular, it suggests that it is possible to do so by exploiting the real-time monitoring and analysis of digital twins, combined with innovative crisis simulations, as well as leveraging collaboration strategies and the combined deployment of digital twins together with other key supporting technologies and data infrastructures.

The solution discussed in this paper consists of the creation of a digital twin at a much broader scale compared to what has been implemented so far. It consists of pooling together a massive amount of data which can support the monitoring of supply chain processes in both conflict time and in peacetime, for higher preparedness and resilience. This is achieved through a digital ecosystem monitoring production, shipments and stocks of critical goods which pools together data from a myriad of sources. Such data mass at the moment is not available or only partially, so it is suggested to create synergies with the Common European data spaces that are currently being launched in multiple domains by the EU. This would also allow the establishment of a ‘modular’ digital twin which can be plugged into a specific data space to retrieve data. This would be also beneficial for multiple reasons: i) obtain data at the necessary level of quality/granularity, ii) benefit from the governance and security requirements already in place, iii) benefit from decentralised computing.

Considering the current state and the expected growth in both high-quality data availability and computing capabilities, it is reasonable to assume a gradual development of this digital twin solution throughout the next two decades. In terms of computing capabilities, the current capabilities can already allow the digital twin not only for accurate descriptive analysis of the current environment and for conducting predictive modelling, but also for scenario planning and simulation. However, the real goal would be to move towards operational excellence based on real-time data integration through AI in control towers and possibly synced with advanced MX-based or XR-based data visualisation.

Meanwhile, with regards to data availability, this represents the main issue and highest efforts should be put in boosting it, both on the technical side and on the policy side. By the end of this decade, on the civilian side it can be expected that the first common EU data spaces will become operational and provide data useful for descriptive analysis and predictive modelling. On the military side, the same capabilities can be achieved if every country (individually or in joint ventures) starts the development of its own digital twins by pooling together data from warehouses and barracks, repair and training sites, ports/airports/missile sites, etc. This would be followed by extending the supply chain data flows, by plugging-in data from the defence industry. The result would be a ‘defence data space’ to be subsequently connected with other Common European data spaces (e.g. manufacturing) to complement the virtual supply chain with further data on other goods (e.g. medical supplies), energy and raw materials availability.

References

Bellamy III, W., (2018). Boeing CEO Talks 'Digital Twin' Era of Aviation. *Aviation Today*. Available at: https://www.aviationtoday.com/2018/09/14/boeing-ceo-talks-digital-twin-era-aviation/ [Accessed: 26/3/2023]

Bécue, A., Maia, E., Feeken, L., Borchers, P., & Praça, I. (2020). A new concept of digital twin supporting optimization and resilience of factories of the future. *Applied Sciences*, *10*(13), 4482.

European Defence Agency (2022a). *EDM Issue #23, EU's Strategic Compass / Follow the Ambition*. Available at: https://eda.europa.eu/docs/default-source/eda-magazine/full-edm-23-(final).pdf. [Accessed: 15/3/2023]

European Defence Agency (2022b). *EDM Issue #24, Investing in European defence today's promises, tomorrow's capabilities?,* Available at: https://eda.europa.eu/docs/default-source/eda-magazine/edm24final.pdf. [Accessed: 15/3/2023]

Fiott, D. The Fog of War: Russia's War on Ukraine, European Defence Spending and Military Capabilities. Intereconomics 57, 152–156 (2022). https://doi.org/10.1007/s10272-022-1051-8 [Accessed 28/3/2023]

Holmes, D., Papathanasaki, M., Maglaras, L., Ferrag, M. A., Nepal, S., & Janicke, H. (2021, September). Digital Twins and Cyber Security–solution or challenge?. *In 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)* (pp. 1-8). IEEE.

Katsaliaki, K., Galetsi, P. & Kumar, S. Supply chain disruptions and resilience: a major review and future research agenda. *Ann Oper Res* 319, 965–1002 (2022). https://doi.org/10.1007/s10479-020-03912-1 [Accessed: 26/3/2023]

Mendi, A.F., Erol, T., and Doğan, D. (2022). *Digital Twin in the Military Field*, in IEEE Internet Computing, vol. 26, no. 5, pp. 33-40. Available at: https://ieeexplore.ieee.org/document/9345490. [Accessed: 19/3/2023]

Sani, S., Schaefer, D., & Milisavljevic-Syed, J. (2022). *Utilising Digital Twins for Increasing Military Supply Chain Visibility*. Available at: https://eprints.lincoln.ac.uk/id/eprint/50348/. [Accessed: 15/3/2023]

Sani, S., Schaefer, D., Milisavljevic-Syed, J. (2022), *Strategies for Achieving Pre-emptive Resilience in Military Supply Chains*, Procedia CIRP, Volume 107, Pages 1526-1532, Available at: https://doi.org/10.1016/j.procir.2022.05.186. [Accessed: 28/3/2023]

Stoetman, A., (2023), European Security and Defence: Don't Get Your Hopes Up Just Yet. In *IAI Commentaries 23|09 - March 2023*. Available at: https://www.iai.it/sites/default/files/iaicom2309.pdf [Accessed 28/3/2023]

Wu, J., Yang, Y., Cheng, X. U. N., Zuo, H., & Cheng, Z. (2020, November). The development of digital twin technology review. In *2020 Chinese Automation Congress (CAC)* (pp. 4901-4906). IEEE.

Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Paving the last mile of artificial intelligence with edge computing. *Proceedings of the IEEE*, *107*(8), 1738-1762.