



GUIDE DEFENCE · 9 MIN READ

Resilient supply chains in the defence industry

Forward manufacturing, decentralisation and supply chain resilience: why the defence industry is rethinking its supplier structures.

The vulnerability of global supply chains

The COVID-19 pandemic, the war in Ukraine and geopolitical tensions in the Indo-Pacific have laid bare the vulnerability of global supply chains. In the defence industry this vulnerability weighs particularly heavily: if critical materials or components are unavailable, weapon systems cannot be produced, serviced or repaired — with immediate consequences for defence capability.

- Raw material dependency: rare earths (China), titanium (Russia/Ukraine), tungsten (China) — strategic materials with concentrated supply chains
- Single-source risks: many defence components have only one qualified supplier — if that supplier fails, production comes to a standstill
- The just-in-time problem: lean production does not work under wartime conditions — stockholding is becoming strategically important again
- Geopolitical risks: trade embargoes, export restrictions and technology blockades can interrupt supply chains overnight
- Cyber risks: attacks on suppliers' IT systems can paralyse the entire value chain

Note: Case study: the titanium crisis — Until 2022 the European aerospace industry sourced a considerable share of its titanium from Russia (VSMPO-AVISMA). Sanctions forced a switch to alternative sources at short notice — with price increases of over 40 % and delivery delays of months. The defence industry responded with stockholding programmes and the qualification of new suppliers in Japan, the USA and Kazakhstan.

Forward manufacturing and decentralisation

Forward manufacturing — relocating production capacity closer to the point of use — is a central concept in NATO's new defence planning. Instead of manufacturing all weapon systems in a few central plants and transporting them along long logistics chains, regional manufacturing and repair centres are intended to improve security of supply. For specialised suppliers such as refractory companies, this opens up new business models.

- Regional repair centres: the Bundeswehr is planning maintenance hubs close to its stationing locations — short distances, fast repair
- NATO forward deployed manufacturing: production capacity on the eastern flank (the Baltic states, Poland,

Romania) for rapid resupply

- Mobile repair teams: specialised teams carrying out repairs in the field — including for high-temperature components
- Dual sourcing: systematic qualification of at least two suppliers for every critical component
- Reshoring: relocating production back to Europe — particularly for security-critical materials and components

Note: An opportunity for SMEs — Forward manufacturing and decentralisation favour medium-sized companies with a regional presence. A refractory specialist based in southern Germany can supply regional repair centres faster and more flexibly than a large international group. Flexibility, short decision paths and technical expertise are the competitive advantages of SMEs.

Stockholding and the strategic reserve

The return to national and alliance defence has put the question of stockholding back on the agenda. Ammunition, spare parts and critical materials must be stockpiled in sufficient quantities so as not to depend on functioning supply chains in the event of a conflict. For suppliers this means long-term framework agreements with guaranteed call-off volumes — an attractive business model.

- Ammunition stockpiling: NATO has raised its stockholding targets sharply — from 30 to 60+ days of combat supplies
- Spare parts pools: central and decentralised stores for critical spare parts — including components for furnaces and energy systems
- Framework agreements: long-term supply agreements (5–10 years) with guaranteed minimum and maximum quantities
- Emergency ramp-up plans: suppliers must demonstrate that they can scale up their production at short notice in a crisis
- Strategic raw material reserve: stockpiling titanium, tungsten, rare earths and other critical materials

Recommended actions for suppliers

The realignment of defence supply chains offers concrete options for action for medium-sized suppliers. Companies that position themselves strategically now can benefit from these structural changes over the long term.

- Supply chain analysis: identify your own dependencies — raw materials, intermediate products, logistics. Prepare supply chain documentation for defence customers
- Offer dual sourcing: position yourself as an alternative to existing single-source suppliers — actively offer to undergo qualification
- Build up storage capacity: signal your willingness to stockpile critical materials — offer warehousing as a service
- Develop an emergency ramp-up plan: document how production can be doubled or tripled at short notice in a crisis
- Cyber security: implement IT security standards (ISO 27001 as a minimum) — defence customers increasingly scrutinise their suppliers' cyber security

Note: Quick win: supply chain transparency — Produce a documented overview of your own supply chain: where do your raw materials come from? Are there any single-source dependencies? How long will your stocks last? Defence buyers ask for precisely this information. Being able to present it proactively is a competitive advantage.

Frequently asked questions

As a supplier, do I have to build up my own stockholding?

Not necessarily, but a willingness to do so is a competitive advantage. Many defence framework agreements contain clauses on minimum stockholding. The cost of warehousing is generally covered by the contract price. For a refractory company this could mean holding critical materials (corundum castables, special bricks) for 3–6 months of production.

What is meant by an emergency ramp-up plan?

An emergency ramp-up plan documents how a company can increase its production at short notice in a crisis: additional shifts, reserve capacity, pre-qualified agency staff, access to raw material reserves. Defence customers expect this plan as part of supplier qualification. It must be realistic and workable — a mere declaration of intent is not enough.

Which cyber security standards are expected of defence suppliers?

As a minimum, implementation of the BSI IT-Grundschutz baseline protection or ISO 27001. Suppliers with access to classified information are additionally subject to the BSI's guidelines for classified IT. The USA requires its suppliers to hold CMMC (Cybersecurity Maturity Model Certification) — relevant for companies supplying US programmes.

Let us talk about your project

Reply within 24 hours on working days.

info@sbs-rs.de

+49 89 541 960 209 Read online: www.sbs-rs.de/defense-industrie/ratgeber/resiliente-lieferketten-defense