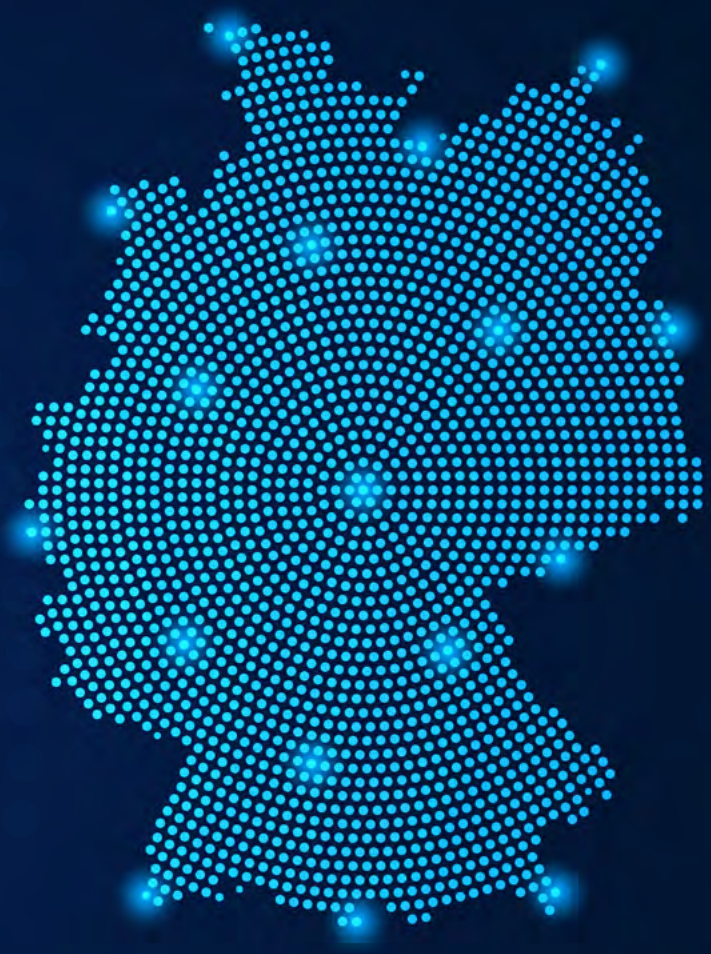
zentrum Nachhaltige Transformation
an der Quadriga Hochschule Berlin

MHP
A PORSCHE COMPANY

bwconsulting



STUDY

Private Sector–Military Cooperation for a Defensible and Resilient Germany

German Logistics Hub

A study by:
zentrum Nachhaltige Transformation (Center for Sustainable Transformation) at Quadriga Hochschule Berlin
BwConsulting GmbH – the in-house consultancy of the Bundeswehr
MHP Management- und IT-Beratung GmbH

Berlin, November 2025

Executive Summary

How can the Federal Republic of Germany structure the cooperation between the Bundeswehr (German federal armed forces) and the private sector within the framework of private sector–military cooperation (PMC) in such a way that Germany's defense capability and resilience are enhanced?

Since the annexation of Crimea in 2014, and increasingly due to the full-scale Russian invasion of Ukraine since 2022, Germany has faced new security policy challenges. These challenges cannot be mastered purely militarily; they must be addressed on a national and societal level. Germany has transformed from a potential battleground of the Cold War into the logistical backbone for NATO (German hub) – troops and materials of the alliance partners must be transported quickly and reliably from west to east in case of tension or conflict, and soldiers need to be supplied.

The "Operations Plan Germany (OPLAN DEU)" of the Bundeswehr consolidates the central military components of national and alliance defense in Germany with the necessary civilian support services into an operationally executable plan. OPLAN DEU is thus, among other things, the basis for military planning for the establishment of the hub in Germany. The details of the operations plan are secret, but some principles are known and part of the public discussion. It is clear that the private sector must play a central role in addressing the logistical challenges within the framework of OPLAN DEU and the German hub. Germany's companies are ready for such cooperation, but there is still a lack of necessary information for the effective establishment of the hub and thus effective implementation of OPLAN DEU due to strict confidentiality.

Against this backdrop, our study addressed the following key question: How can the Federal Republic of Germany structure the cooperation between the Bundeswehr and the private sector within the framework of private sector–military cooperation (PMC) in such a way that Germany's defense capability and resilience are enhanced? For this purpose, the study addressed three central questions:

1. Which challenges must be overcome?

The threat situation requires a new, more intensive cooperation between all societal and state sectors, far beyond the Bundeswehr and the private sector. The concept of "Comprehensive Defense" on the one hand highlights the complexity of the task, and on the other hand makes it immediately clear that, among other things, the sub-area of PMC should be coordinated quickly and efficiently in order to achieve seamless processes and the effective use of available resources in the face of many challenges. Speed and effectiveness are the order of the day.

However, this discussion is not primarily about the question of which ministry and which authority should be responsible for which task in the future. As the concept of "Comprehensive Defense" shows, the question of the overall architecture is crucial. The focus should be on functionally integrating the different tasks within defense, not on coordinating them institutionally.

2. What best practices can Germany learn from?

Some NATO member states have already developed proven models for a PMC at the interfaces between the state, military, and private sector actors. Germany can take advantage of these experiences:

1. State coordination:

Clear responsibilities on the part of the state are necessary to inform the actors about their tasks, to effectively manage their efforts, and to gain an accurate overview of the situation.

2. Binding structures:

The responsibilities must of course be supplemented by a structural and procedural organization to optimize cooperation.

3. Incentives:

Incentive and hedging mechanisms for the participating private sector actors are necessary to secure their investments and engagement.

The private sector, in turn, has a number of proven solutions, especially for logistical tasks, to meet the challenges for a "German hub":

→ Advanced digitization is used daily by companies to control and monitor logistics processes;

→ Digital platforms, tracking systems, and automated planning processes continuously provide a real-time overview of available resources, routes, and bottlenecks;

→ Not least due to crises such as the Russian full-scale invasion of Ukraine, companies have significantly increased the resilience of their supply chains and are able to respond quickly and appropriately to problems.

The example of the Convoy Support Centers, for which the Bundeswehr commissioned the company Rheinmetall for 263 million euros, demonstrates exemplary solutions for a new form of PMC that needs to be expanded and systematized.

3. What could an exemplary solution for the German hub look like?

The study suggests developing a "German Digital Logistics Hub." At the center of this system is a digital twin of private sector logistics. It provides – based on the data that companies are already using today – a real-time overview that makes all available resources and services of private sector providers transparent and enables not only a situational picture, but also the concrete control of individual activities. Such a digital twin also creates the necessary transparency and legally binding nature for the PMC.

Next steps

The authors see the study as a contribution to supporting the enormous challenges in establishing the "German hub" with concrete proposals – from shaping the legal framework to setting up a comprehensive logistical system. In doing so, we rely on existing concepts to address national and societal challenges ("Comprehensive Defense"), reference experiences in other NATO countries in the area of PMC, and ultimately recommend the use of already tested, functional solutions from the private sector. This is necessary given the security

policy situation, and all the more appropriate in view of the goals of speed and effectiveness in the approach.

In the next step, our aim is to familiarize the political, administrative, and military decision-makers with the possibilities of PMC and their opportunities, and to encourage them to test the proposed model.

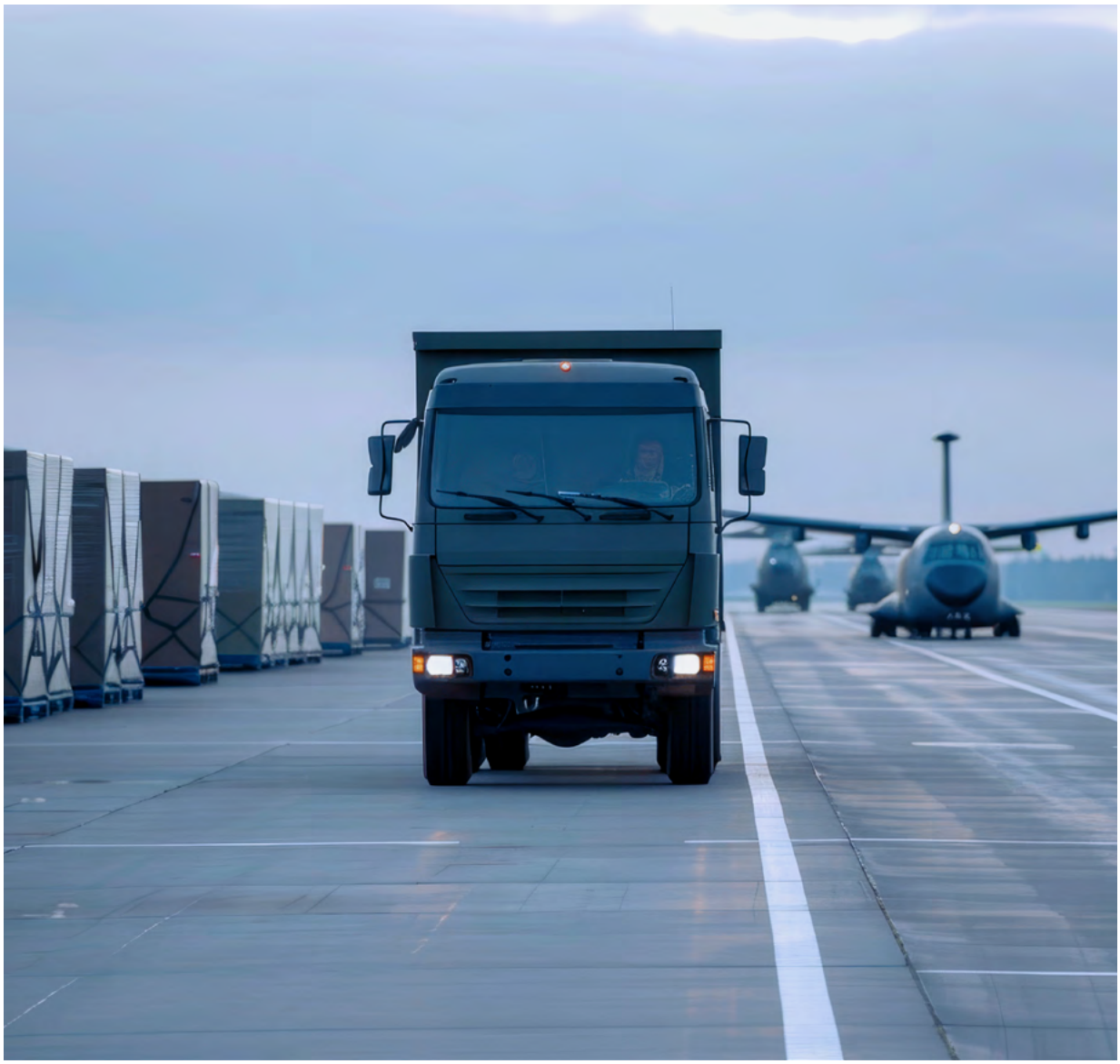


Table of Contents

Authors of the Study

This study was created as part of a project collaboration between the zentrum Nachhaltige Transformation at Quadriga Hochschule Berlin, BwConsulting GmbH – the in-house consultancy of the Bundeswehr, and MHP Management- und IT-Beratung GmbH.

zentrum Nachhaltige Transformation (Center for Sustainable Transformation) at Quadriga Hochschule Berlin

Prof. Dr. Torsten Oltmanns
Dr. Ute Preusse-Hüther
Julia Irina Rosenkranz
Cornelia Rülke
Benjamin Kupke

BwConsulting GmbH – the in-house consultancy of the Bundeswehr

Michael Rogasch, Managing Director
Daniel Bitter, Principal
Manfred Husa, Manager
Jonathan Ponfick, Consultant

MHP Management- und IT-Beratung GmbH

Henning Schulze, Partner
André Wilke, Associated Partner
Cihan Sügür, Associated Partner
Stefan Meinecke, Associated Partner
Stephan Martin, Associated Partner
Florian Adolf, Senior Manager
Joerg Schmidt-Romm, Senior Manager
Dr. Michael Bauer, Senior Manager
Marius Pudeg, Senior Consultant

List of Abbreviations

AJP-4 – Allied Joint Publication 4 (NATO Principles and Policies for Logistics)
Bw – Bundeswehr
CEF – Connecting Europe Facility
CER – Critical Entities Resilience Directive
CSC – Convoy Support Center
EU-TEN-T – Trans-European Transport Network
FSC – Facility security clearances
FüInfoSys – Command information system
HAbt – Main department
HNS – Host nation support
KRITIS – Critical infrastructures
LMS-V – Logistics Management System Defense
LOGFAS – Logistics Functional Area Services (NATO logistics software)
MSB – The Swedish Civil Contingencies Agency
MoFIS – Mobility Management Information System of the Bundeswehr
NATO – North Atlantic Treaty Organization
NCTV – Dutch National Coordinator for Counterterrorism and Security
NESA – National Emergency Supply Agency
NFM – NATO Force Model
NIS2 – EU Directive on measures for a high common level of cybersecurity (2022)
OPLAN DEU – Operations Plan Germany
PMC – Private sector–military cooperation
SASPF – Standard Application Software Product Families (Bw IT system)
STANAG – NATO Standardization Agreement
STUFT – Ships Taken Up From Trade (Merchant ships for military purposes)
UstgKdo – Support Command
CIMIC – Civil–military cooperation

1. Introduction

Germany has concretized part of its new role in the Operations Plan Germany (OPLAN DEU). The goal is to enable NATO troops to quickly provide a flexible and effective response in the event of threats or need for defense through adequate preparation.

1.1 Turning point in security policy

The security policy situation in Europe has fundamentally changed since the annexation of Crimea in 2014 and especially due to the full-scale Russian invasion of Ukraine in 2022. Germany thus faces new challenges in national and alliance defense and assumes a central role in the European security structure as a NATO member:

Germany is changing from a potential combat zone to a logistical hub. Against this backdrop, NATO has developed new (regional) defense plans. Germany has concretized part of its new role in the Operations Plan Germany (OPLAN DEU). The goal is to enable NATO troops to quickly provide a flexible and effective response in the event of threats or need for defense through adequate preparation.

The Bundeswehr cannot fulfill these requirements alone. In view of its limited own resources, it is highly dependent on support from the private sector – particularly in the areas of logistics, IT, and infrastructure. This makes structured integration of private sector and military capacities a decisive success factor for the defense capability of Germany and the alliance.

1.2 Objective of the study

Against this background, the present study examines how an effective and robust cooperation between the Bundeswehr and the private sector can succeed in the context of OPLAN DEU. OPLAN DEU is the national operations plan that describes how Germany ensures its contribution to national and alliance defense within the framework of NATO defense planning, including military, civilian, and private sector contributions to support allied forces on German soil. The framework condition is that OPLAN DEU is not publicly accessible. The basic principles are, however, known and part of security policy communication. This study utilizes publicly accessible information and known guidelines of OPLAN DEU.

The focus of the study is on the question of under what conditions and with what implementation private sector services – particularly logistical, digital, and organizational competencies – can be planned, reliably integrated, and managed. In addition to the publicly known objectives of OPLAN DEU, especially ensuring national and alliance defense in Germany, NATO planning simultaneously assumes the necessity of relocating and supplying up to approximately 800,000 soldiers[1] along with material and equipment within up to six months across German territory in the event of a crisis or defense situation – a magnitude that clarifies the scale of civilian and private sector requirements.

[1] Bundeswehr, Operations Plan Germany (OPLAN DEU): Deutschland gemeinsam verteidigen, online: https://www.bundeswehr.de/de/organisation/operatives-fuehrungskommando-der-bundeswehr/auftrag-und-aufgaben/operationsplan-deutschland (accessed October 28, 2025).

The study first considers the security policy context, the significance of OPLAN DEU, and Germany's role as a logistical hub. Subsequently, general requirements for effective cooperation between the Bundeswehr and the private sector are defined, considering the logistics requirements of NATO. International PMC models are then analyzed and best practices identified. Based on the analyses of the general requirements as well as international best practices, derivations and recommendations for action for Germany are formulated.

Against this background, the study examines best practices from the private sector that illustrate how the private sector effectively addresses existing logistical challenges and where cooperation potentials lie. In addition, the study formulates, taking into account the defined best practices and prerequisites, an exemplary solution approach for a German Digital Supply Hub. This model aims to link military needs with private sector services and to create a common situational picture that enables the planned activation and controllability of private sector services in crisis and defense situations. The concept is a digital private sector–military logistics platform that ensures appropriate implementation through interoperable interfaces, modular functional components, and differentiated role logics.

Central interim results, assumptions, and the exemplary solution approach of the German Digital Supply Hub were reflected in technical discussions with representatives of the Bundeswehr. This feedback served to validate the findings and ensure the practical applicability of the recommendations.

1.3 Project partners

The present study is a joint project of the "center for sustainable transformation" (zNT) at Quadriga Hochschule (University of Applied Sciences) Berlin, BwConsulting – the in-house consultancy of the Bundeswehr, and the management and IT consultancy MHP. Through the complementary expertise of the involved partners, both scientifically analytical and practice-oriented perspectives on private sector–military cooperation are considered.

zentrum Nachhaltige Transformation – Quadriga Hochschule Berlin

The zNT is a consultancy and think tank at the Quadriga Hochschule (University of Applied Sciences) in Berlin, with extensive experience in consulting on transformation processes as well as a strong scientific and practice-oriented network. The zNT brings its scientific expertise to the analysis and simultaneously supports the transfer of results to politics, professional circles, economic activity, and the public.

BwConsulting GmbH – the in-house consultancy of the Bundeswehr

As the in-house consultancy of the Bundeswehr, BwConsulting acts as a bridge between military practice and strategic development. BwConsulting uses its deep and specific customer knowledge, developed continuously over many years, in the Bundeswehr, and appropriately links it with contemporary and innovative management trends and innovations. With its experience in transformation projects within the Bundeswehr, BwConsulting is the right partner when it comes to managing the complexity of the future, identifying opportunities and risks, and leveraging the best expertise from all areas in practical solutions for the Bundeswehr through transformative partnerships.

MHP Management- und IT-Beratung GmbH

MHP is an internationally active consulting company with many years of expertise in digitalization, processes, and logistics. As a 100%-owned subsidiary of Porsche AG and part of the Volkswagen Group, MHP combines deep industry and transformation knowledge with practical experience in complex supply chains. In the study, MHP brings the perspective of the industry – particularly with regard to the digital management and efficiency enhancement of logistical processes.

2. Background

Germany is in a new security policy reality: from the potential conflict zone to NATO's logistics hub.

2.1 Germany's security policy realignment under changed conditions

Germany is facing a new security policy reality. Both state and non-state actors are increasingly acting aggressively in the information space, in cyberspace, and through economic dependencies – with the aim of weakening our stability, capacity to act, and social cohesion.

These actors use a variety of means to pursue their goals. The threat or even the use of military force is just the tip of the iceberg. Hybrid attacks, such as cyberattacks, disinformation campaigns, and covert activities by agents have become part of our reality. Targets are no longer only national security institutions such as the police, military, or intelligence services, but also critical infrastructures (KRITIS) like airports, power, gas, and hydroelectric plants, and the private sector. The manner of the attacks poses new challenges to the Federal Republic of Germany, which has divided its areas of action into clearly definable and separable areas through the principle of departmentalization and federalism in its responses. This has led to new perspectives in politics and society. The National Security Strategy[2], the framework guidelines for Comprehensive Defense[3], and the Defense Policy Guidelines[4] take this new reality into account. They are action-guiding for the relevant stakeholders, but must first be operationalized in practice to fully take effect.

Germany began precisely this operationalization in 2022, when Chancellor Olaf Scholz declared the turning point following Russia's full-scale invasion of Ukraine. The intention is to make the Bundeswehr (Bw) capable of defense again with a special fund of 100 billion euros. However, it quickly became apparent that this amount would be sufficient neither for the retrofit nor for its maintenance. After Donald Trump was re-elected in 2024, the Federal Republic of Germany was forced to make further adjustments. With the relaxation of the debt brake for defense expenditures, the path was clear to provide the Bundeswehr with additional resources. However, the rearmament of the Bundeswehr faces a multitude of challenges. The military capability in 2029 is stipulated as a guiding principle[5], and even the reintroduction of conscription is not considered impossible, although a new, voluntary-based military service model has been agreed upon for the time being.[6] On the other hand, the security and defense industry has been treated as a societal non-player for many years and has reduced capacities, even though this trend has been slowly but steadily changing since 2022.

At the same time, the German private sector faces equally significant challenges. The increasing protectionism of the USA and China, coupled with the loss of Russian energy, has shaken the foundations of the German business model. The German private sector must maintain existing sales markets under new customs regimes, open up new sales markets,and additionally remain strong in innovation to compete in a competitive global market. Only strong economic activity can provide the means and resources that Germany needs to guarantee its security militarily. The integration of economic and military security is an expression of the changed security policy reality; however, awareness of the operational impacts of this integration is insufficient on both sides. To reduce the disadvantages of federalism and the departmental principle in Germany, all institutions need a joint conceptual framework.

[2] German Federal Government: National Security Strategy of the Federal Republic of Germany, online: https://www.nationalesicherheitsstrategie.de/ (accessed October 28, 2025).

[3] German Federal Ministry of the Interior (BMI): Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien (RRGV), online: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/RRGV.html (accessed October 28, 2025).

[4] German Federal Ministry of Defence (BMVg): Defence Policy Guidelines 2023, online https://www.bmvg.de/de/aktuelles/verteidigungspolitische-richtlinien-2023-veroeffentlicht-5701338 (accessed October 28, 2025).

[5] Deutscher Bundestag: Regierungsbefragung im Wortlaut, June 5, 2024, online: https://www.bundestag.de/dokumente/textarchiv/2024/kw23-de-regierungsbefragung-1002264 (accessed October 28, 2025).

[6] BMVg: Neuer Wehrdienst für Deutschland, online: https://www.bmvg.de/de/neuer-wehrdienst (accessed October 28, 2025).

2.2 Comprehensive Defense as a conceptual framework

With the National Security Strategy (NSS) as the top security policy umbrella document, the Federal Government aims to promote a continuous process of cooperation among all state levels, the economy, and society for the security of Germany (Policy of Integrated Security). [7] In the current security policy situation, it is simply no longer sufficient to understand security and resilience solely as military defense. Security today is complex and interconnected and can only succeed on a societal and governmental level.

In order to appropriately address the demands arising from this fundamentally comprehensive understanding of politics, it is necessary, even beyond the strategic or conceptual foundations based on the NSS (Defense Policy Guidelines/BMVg, Civil Defense Concept/BReg, Comprehensive Defense Framework Directive/BMI), to develop concrete, holistic solutions. An organizing structure that concretizes Integrated Security or the comprehensive societal and state approach across institutional boundaries is essential. The purpose of such a structure would initially be to promote a uniform understanding of key terms and concepts as well as a common language among all relevant stakeholders. In the end, it is primarily about implementing Integrated Security, i.e., supporting a holistic operationalization of solution spaces as well as the planning, implementation, and prioritization of concrete measures.

Such a structure can ultimately serve as the basis for effective complexity management in terms of an architecture by ideally representing the connecting logic from the political to the strategic and operational level (vertical structure) and depicting functional interrelationships at one level (horizontal structure).

A concept[8] that provides this is the Comprehensive Defense for Germany[9] framework by BwConsulting. Within this framework, it is necessary to understand defense in Germany comprehensively. It organizes the aspects of state, economy, and society that contribute to Integrated Security into seven segments:

[7] German Federal Government: National Security Strategy of the Federal Republic of Germany, online: https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf (accessed October 28, 2025), p. 18, 28 ff

[8] The framework adopts approaches from other (NATO) states, as well as from the Cold War era (e.g., the concept of Total Defense in Finland and Sweden) and also from NATO, and has adapted and further developed them based on the current threat situation, including NSHQ 2020, Comprehensive Defence Handbook, Volume 2 or SHAPE 2023, Comprehensive Operations Planning Directive.

[9] BwConsulting: Landes- und Bündnisverteidigung – Framework Comprehensive Defence für Deutschland, online: https://www.bwconsulting.de/lvbv (accessed October 28, 2025).

Figure 1: Comprehensive Defense overview

The framework maps the complexity of the defense landscape and its diverse connections and interfaces, and provides the complex challenges of Integrated Security with a deliberately functional rather than an institutional structure. Together, the segments form the shield of a comprehensive defense. Every single segment is important to ensure the security and ability of the state to act. If a segment is not sufficiently strong, the shield not only loses its protective effect at that one point. Rather, the stability of the entire shield is weakened.

The core of the present study is the Military Defense segment. Nevertheless, the added value of the framework lies beyond considering individual segments, but rather in identifying intersegment correlations or interactions and a holistic view. The goal is to contribute to comprehensive planning and management that meets the demands of an overall societal approach. This is because the security of Germany is ensured not only by the Bundeswehr, but also by the preservation of natural resources and social cohesion, on which a democracy relies more than any other form of government.

To what extent does the present study contribute to a cross-segment viewpoint? How is the interaction between the Bundeswehr and the private sector to be understood within the framework of Comprehensive Defense?

OPLAN DEU combines the central military components of national and alliance defense in Germany with the necessary private sector support services into an operationally executable plan. Maximum private sector support is a crucial factor in OPLAN DEU. The operations of the armed forces, especially in times of crisis and war, particularly their endurance, depend on a resilient and efficient economy. To ensure the latter, stable supply chains and a secured energy and raw material supply are also necessary. This interaction must be actively shaped by a multitude of institutions at various levels. Both sides of this causal relationship must be able to meet the needs of the other, which requires congruent, integrated planning and control, effective communication, reliable data exchange, and also practical interaction. The Comprehensive Defense framework not only provides a means of managing complexity, but also connects a functional, impact-oriented perspective with the institutional view (form follows function).

2.3 Challenges

The North Atlantic Treaty Organization (NATO) as the central defense alliance of the Federal Republic of Germany responded to the changed security situation due to the Russian full-scale invasion of Ukraine in 2022 and decided on new regional defense plans at its summit in Vilnius in 2023.[10] Although these plans are secret, it is assumed that depending on the threat situation and escalation, up to 800,000 soldiers[11] will be mobilized to deter or repel a threat. These defense plans concern the allied forces of all NATO members.[12]

[10] NATO: Topic: Strengthening NATO's eastern flank, online: https://www.nato.int/cps/en/natohq/topics_136388.htm (accessed October 28, 2025).

[11] Bundeswehr, Operations Plan Germany (OPLAN DEU): Deutschland gemeinsam verteidigen, online: https://www.bundeswehr.de/de/organisation/operatives-fuehrungskommando-der-bundeswehr/auftrag-und-aufgaben/operationsplan-deutschland (accessed: October 28, 2025).

[12] BMVg: Zeitenwende – Grundsatzdokumente und strategische Neuaufstellung, online: https://www.bmvg.de/de/themen/sicherheitspolitik/zeitenwende (accessed October 28, 2025); BMVg: NATO Force Model – Wie Deutschland sich ab 2025 engagiert, online: https://www.bmvg.de/de/aktuelles/nato-force-model-wie-deutschland-sich-ab-2025-engagiert-5465714 (accessed October 28, 2025); Stiftung Wissenschaft und Politik (SWP): Die Nato nach dem Gipfel von Madrid, SWP-Aktuell 2022/A 49, online: https://www.swp-berlin.org/10.18449/2022A49/ (accessed October 28, 2025).

This raises the question: When Bundeswehr units and allied forces are to be deployed to the eastern flank to deter or repel a Russian threat, who plans and conducts the transport to the deployment areas?

In order to be able to answer these and other questions, the Bundeswehr, together with other relevant actors from the federal government, states, and municipalities, have developed the Operations Plan Germany (OPLAN DEU) and continuously update it. OPLAN DEU specifies, among other things, how the allied forces can reach their designated deployment areas across Germany. It is becoming clear that Germany will be the central logistics hub and must prepare for this.

The Bundeswehr currently lacks sufficient logistical capacities to meet this great challenge because they were largely reduced and dissolved in the Bundeswehr reforms of the 2000s and 2010s. The resources available are needed by the Bundeswehr for its own deployment and stationing in Eastern Europe.

It must therefore be assumed that other actors in the Federal Republic of Germany will have to tackle the logistical challenges of the deployment of NATO units to the deployment area. This challenge of relocating up to 800,000 soldiers along with equipment and heavy machinery, as well as the repatriation of injured and fleeing individuals, can only be solved on this scale through cooperation with civilian and private sector actors (known as civil–military cooperation, CIMIC):

> "CIMIC describes the cooperation between governmental or non-governmental civilian organizations and the armed forces in the realm of alliance and national defense, in hazard prevention, in disaster relief, or in overseas deployments of the armed forces as part of stabilization operations or humanitarian missions."[13]

While the Bundeswehr and civilian organizations such as the emergency services or the Federal Agency for Technical Relief (THW) regularly collaborate, this is not the case for most private sector actors – there is still need for regulation or action in this area. Since the Federal Republic of Germany will be reliant on cooperation with these actors, the study will focus on private sector–military cooperation (PMC) as a subset of CIMIC.

[13] German Federal Office of Civil Protection and Disaster Assistance (BBK): Zivil-Militärische Zusammenarbeit, online: https://www.bbk.bund.de/DE/Themen/Krisenmanagement/Zivil-Militaerische-Zusammenarbeit/zivil-militaerische-zusammenarbeit_node.html (accessed October 28, 2025).

2.4 Private sector–military cooperation

For this study, PMC is defined as the contractual integration of private companies (including in the areas of logistics/transport, IT) for the operational support of the Bundeswehr. During the Cold War, the Bundeswehr had significantly more of its own material and personnel resources available for these activities, in addition to extensive standby contracts with private sector actors, such as freight forwarders, than is currently the case. Moreover, the fundamental military situation was different: Back then, Germany was a potential combat zone[14]; today it is primarily a logistical hub.

The formerly existing logistical structures and resources made available were dismantled or even completely dissolved as part of the shift in the Bundeswehr's priority from national and alliance defense to international crisis management, and the reorganizations of the 2000s and 2010s. The renewed focus on national and alliance defense now requires a similar amount of resources, though without being able to rely on the same structures. These circumstances can be addressed by increased PMC.

The German economy can provide a large amount of resources that the Bundeswehr, or in the broader societal context of Comprehensive Defense, the Federal Republic of Germany, needs to fulfill its mission in the context of national and alliance defense.

For this reason, the present study will address the following question:

How can the Federal Republic of Germany structure the cooperation between the Bundeswehr and the private sector within the framework of private sector–military cooperation (PMC) in such a way that Germany's defense capability and resilience are enhanced?

[14] Bundeswehr Centre of Military History and Social Sciences (ZMSBw): Schichttorte Vorneverteidigung Kalter Krieg, online: https://zms.bundeswehr.de/de/mediathek/aktuelle-karte-schichttorte-vorneverteidigung-kalter-krieg-5533640 (accessed October 28, 2025).

3. Requirements

The effectiveness of private sector–military cooperation is measured by the operational capability, not by efficiency indicators.

To approach this core point, the study defines seven general requirements for successful PMC. These are derived from NATO frameworks, Bundeswehr requirements, and experiences from past crises:

1. Primacy of operational requirements: effectiveness before efficiency	In successful PMC, the fulfillment of operational requirements must take priority. The primary objective of PMC must be effectiveness, while ensuring the best possible efficiency.
2. Increase in operational capability	PMC must maximize the capabilities and potential of the deployed forces.
3. Clear control and responsibilities	Clear control mechanisms, responsibilities, and decision-making paths are essential for a functioning PMC.
4. Interoperability and standardization	Clear national standards are a prerequisite for effective PMC.
5. Security and compliance	Security and compliance form the foundation of every PMC.
6. Transparency and information situation: basis for control, situation assessment, and supply chain control	Transparency is a key requirement for effective PMC, serving as a foundation for a shared situational awareness and reliable decisions, both in the political arena and at the operational level.
7. Resilience and redundancy	PMC must also function reliably under extreme conditions in crisis and war situations. Two elements are crucial for this: technical and structural redundancies and proactive, systematically anchored resilience planning.

Table 1: Overview of the requirements for successful PMC

4. International Best Practices

Resilient defense structures are created when cooperation between the state and business is institutionally anchored.

As shown by the existing documents and statements from members of the Bundeswehr, the implementation of OPLAN DEU requires far more than just military planning; it requires effective state coordination beyond the German Federal Ministry of Defence (BMVg) that enables the targeted and reliable integration of the private sector capabilities of a highly developed country like Germany into the national defense system. Especially in logistics, IT, and supply, critical resources and management competencies lie outside the armed forces and with private sector actors.

Other NATO member countries have found different solutions for these challenges. This chapter identifies international best practices from NATO where cooperation between the military and private sector works – be it through institutionalized platforms, legal integration obligations, public–private partnerships, or simulation-based mobilization management. The focus is deliberately not on governmental coordination, but on the question of how other states succeed in systematically integrating private sector capabilities into military tasks, processes, and support.

The selection of best practices is based on criteria that allow for the filtering of those NATO states which exhibit relevant cooperation models and logistical hub functions. The aim is not only to provide an overview of good examples, but also to derive concrete approaches for the implementation of OPLAN DEU – particularly with regard to private sector interfaces, technical integration, and strategic resilience.

4.1 Population

The population examined initially included all 32 member states of NATO, based on the collective defense mandate of the alliance according to Article 5 of the North Atlantic Treaty. In the event of a defense situation, every NATO state is potentially involved – be it as a transit country, logistical support, or support nation in the military rear.

4.2 Logistical hub function in the context of NATO as the first filter criterion

In the next step, the population was narrowed down using a systematic filtering process. The goal was to identify those member states that play a key logistical role in the operational NATO context and also meet NATO's logistical requirements in a framework that provides added value with respect to our central question. Initially, the entire population of NATO member states was narrowed down based on their potential function as a logistical hub for military deployment operations. The goal was to identify those countries that can play a critical role in transit, transshipment, and supply of allied forces within the framework of a collective defense scenario – particularly on the eastern flank.

The evaluation was based on three dimensions that can be operationalized:

1. Geostrategic situation in the NATO area:

Assessment based on typical movement axes in large exercises (e.g., Defender Europe 2021, Steadfast Defender 2024), as well as the documented role of national liaison staffs and deployment centers.

2. Multimodal transport infrastructure with dual-use potential:

Alignment with the EU TEN-T corridor planning, military mobility initiatives, and targeted investments from the Connecting Europe Facility (CEF) program.

3. Availability of logistics-capable nodes with HNS suitability:

Consideration of ports, airports, and rail terminals with documented military use within the NATO or EU framework whose connection to logistic information systems (e.g., LOGFAS) is considered likely.

Examples of included sources

As specific military deployment axes in the NATO context are classified, the analysis was based on publicly accessible documents, infrastructure reports, and evaluations of multinational exercises. Examples of publicly documented sources include, among others:

→ Defender Europe 2021: Poland served as a staging and target area for large-scale NATO troop movements along the eastern flank during this exercise. Several US combat units were relocated through the Frankfurt/Oder–Rzepin railway corridor through Germany towards Polish assembly areas.[15]

→ Cold Response 2022: Norway demonstrated multimodal military logistics along Arctic deployment axes with combined sea/air supply and NATO situational awareness integration during this exercise.[16]

→ EU Military Mobility Action Plan & CEF 2023–2027: Plan for the promotion of strategic corridors in Germany, Poland, Finland, and the Netherlands with an explicit dual-use reference.[17]

Identification of initial states as logistical key players

On this basis, the following ten NATO countries were identified as logistical key players:

[15] U.S. Army: Defender Europe 21 – Solidarity on the Move, online: https://www.army.mil/article/252655/defender_europe_21_solidarity_on_the_move (accessed October 28, 2025).

[16] Defense Logistics Agency (DLA): Logistics across Norway for Cold Response, online: https://www.dla.mil/About-DLA/News/News-Article-View/Article/2124356/logistics-across-norway-for-cold-response/ (accessed October 28, 2025).

[17] European Parliament: EU Military Mobility Action Plan & CEF 2023–2027, EPRS_BRI(2025)775860, online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775860/EPRS_BRI(2025)775860_EN.pdf (accessed October 28, 2025).

Country	Reason for selection
Poland	Main connection corridor to the Baltic States and Ukraine; connection to EU corridors and prioritized CEF funding for rail and road axes (e.g. E30, Via Carpatia).
Netherlands	NATO logistics handling through the Port of Rotterdam and MCC-E Eindhoven; central role in multimodal material transfer; EU coordinator for Military Mobility 2021.
United Kingdom	Atlantic bridging link for US reinforcement; air/sea ports with STUFT advance planning; military use e.g., Fairford, Southampton, Marchwood; starting point for forward presence in Eastern Europe.
Norway	Northern flank security; multimodal nodes in Narvik, Bodø, and Tromsø; military-tested infrastructure within the framework of Cold Response.
Denmark	Geopolitical link between Scandinavia and Central Europe; militarily relevant seaports (Esbjerg, Aalborg); Baltic Sea accesses with NATO relevance.
Finland	NATO accession 2023; dual enhancement of infrastructure in Southern Finland and Lapland; TEN-T connection to Baltic Sea and northeast axes.
Sweden	Supplementary role to the Baltic Sea flank; logistical connection via Göteborg and Stockholm; ongoing integration into NATO transport structures.
Italy	Southern logistical backbone for NATO in the Mediterranean region; multimodal hubs in Taranto, Brindisi, and the Po Valley with direct access to the Balkans and the Middle East.
Turkey	Access point to the Black Sea region; strategic hubs in Mersin and Incirlik; air and sea transport axis for southeastern operational areas.

Table 2: Overview of the reasons for selecting the key players

States without verifiable relevance in the three dimensions of geostrategic position in the NATO area, multimodal transport infrastructure with dual-use potential, and availability of logistics-capable nodes with HNS suitability, including Iceland, Luxembourg, Montenegro, and Albania, were not considered in the further scope of investigation.

The first filter reduced the NATO population to ten countries that can function as logistical hubs under realistic operational conditions. The selection was based on documented infrastructure capabilities, multinational exercise practice, and investment-supported mobility planning within the EU/NATO framework.

4.3 Private sector–military cooperation models as a second filter

Starting with the ten logistical hub states identified in the first step, the second filter involved a qualitative narrowing down to those countries where collaboration between military institutions and private sector actors has been structurally planned and operationally tested.

The aim was to identify those states in which military operational planning and private sector capabilities are intertwined, where cooperation is not only inscribed in strategic papers, but is actually effective in everyday operations or exercises.

Evaluation criteria for the functional maturity level of the PMC

The evaluation was based on four observation categories that reflect the practical development status of the PMC:

1. Operationality of the cooperation:

Are there effective procedures through which military and private sector actors can coordinate in an emergency (e.g., joint situational awareness, defined reporting chains, coordinated mobilization processes)?

2. Depth of private sector integration:

Is the private sector only involved as a supplier, or is it part of strategic planning, decision-making, and exercise scenarios?

3. Degree of institutionalization:

Are there permanent platforms, committees, or interfaces through which cooperation occurs, beyond individual projects or ad-hoc formats?

4. Resilience and redundancy orientation:

Is cooperation not only viewed as a method of reaction to crisis, but also focused on continuity, storage, prevention, and systemic resilience?

Evaluation and selection

Of the ten states considered in the first filter, four countries in particular met these four criteria. They have institutionalized procedures, regular practical implementation of exercises, and functional integration of the private sector into security-related processes:

Country	**Brief Profile**
Netherlands	Whole-of-society approach with high involvement of private operators of critical infrastructures; coordinated crisis management through the National Coordinator for Counterterrorism and Security (NCTV); regular situational and crisis exercises with the private sector.
United Kingdom	Distinct public–private partnership models (e.g., AirTanker for air refueling), STUFT concept for civilian maritime fleets, sponsored reserves, strategic framework agreements with logistics and infrastructure companies.
Finland	Statutorily based system of total defense with binding preparedness agreements; operational control via NESA; distinct exercise culture and cross-sectoral Preparedness Committees.
Sweden	Reactivated total defense concept; clear integration of the economy into planning, staff framework exercises, and regional crisis teams; sectorally structured precautionary and redundancy planning.

Table 3: Brief profiles of the selected best practices

The second filter identified the Netherlands, Finland, Sweden, and the United Kingdom as countries with a high functional maturity level of PMC. These countries show that PMC is successful where it is operationally effective, institutionally anchored, and designed to be resilience-oriented. They serve as a reference framework for the implementation of OPLAN DEU in the further course of the study – particularly with regard to the organizational and technical interface formation between military situation management and private sector provision.

The in-depth analysis of the selected countries can be found in Appendix 2.

4.4 Structural principles of functional PMC

The international analysis shows: Successful PMC does not arise from formal guidelines alone, but through lived, institutionalized practice. The cooperation models observed in the four states studied differ in their administrative logic, but they have recurring functional principles that go beyond national peculiarities.

Five overarching structural principles can be derived from the case studies:

→ Binding governance: In all best-practice states, clear governance structures exist, be it in the form of a central authority (NESA, MSB) or through strategically regulated contract architectures (UK MoD).

→ Legally or contractually regulated roles of the private sector: Companies know exactly what obligations and rights they have in the event of defense being required – and on what basis they are involved.

→ Integration in planning and exercise: Private sector actors are not just suppliers, but structural partners – integrated into scenarios, exercises, and mobilization planning.

→ Central confluence: The basis of all models is a shared situational picture, created through the binding and reliable central recording and coordination of capacities and provision data.

→ Incentive and protection mechanisms: Clear liability regulations, financial incentives, and an understanding of social responsibility are in place in order to ensure companies are willing to engage.

These structural principles make it clear: Institutional, legal, and technical foundations are an important prerequisite for a functioning PMC.

5. Derivation of Recommendations for Action for Germany

A robust defense architecture requires systemic, not sporadic cooperation: functionally integrated, federally connectable.

The analysis of the four international reference countries shows that the functional integration of private sector resources into national defense planning is achieved not through sporadic cooperation, but through systemic, institutionalized mechanisms. For Germany, this results in four specific areas that should be considered within the framework of the OPLAN-DEU implementation:

→ the institutional governance in the federal system,

→ the capacity-capable integration of the economy,

→ the creation of a common situational picture as a basis for decision-making, and

→ the development of a sustainable exercise culture.

5.1 Functional coordination in the federal system: the National Security Council as an integration platform

The decision to establish a National Security Council (Nationaler Sicherheitsrat – NSR) and a National Situation Center from 2026 could for the first time create a permanent structure to consolidate security-relevant information across departments and feed it into nationwide decision-making processes. This development provides an important basis for functionally representing the synchronization required between the federal government, states, economy, and military stakeholders as part of OPLAN DEU.

In the sense of the Comprehensive Defense Framework, it is less about institutional control and more about functional integration: A central, shared situational picture forms the prerequisite for creating cross-departmental coherence – without restricting the independence of individual departments or federal levels. In this context, the NSR could not take on an operational leadership role, but would function as an integration platform that brings together information, needs, and priorities from different areas.

That means:

→ Centrality arises from joint situational assessment and strategic prioritization, not from authority to issue directives.

→ Decentralization is maintained through the operational responsibility of the departments and states – they continue to be responsible for planning, implementation, and resource management within their area of competence.

Thus, the NSR Situation Center could become the hub of a federally connectable information and coordination network that brings together military needs (BMVg), civil protection tasks (BMI), economic capacities (BMWK), and federal perspectives. This functional coupling would make it possible to plan across departments without changing the established structures of responsibility.

The model thus follows the basic idea of the Comprehensive Defense Framework: Security is not created by new institutions, but by networked functions. What is crucial is that central situational pictures create transparency, while decentralized implementation competencies remain capable of acting.

5.2 Integration of business with ready availability: the private sector as an institutionalized defense partner

Up to now, involvement of private sector actors in Germany's security preparedness has been sectorally fragmented, partly limited to disaster relief, and legally only sporadically supported (e.g., by the Civil Protection and Disaster Relief Act, the BSI Act, or sectoral security regulations). However, the international analysis shows that resilience primarily depends on early, legally clear, and operational integration of private sector service providers.

What is required is the establishment of a cooperative readiness model that identifies, maintains, and makes capacities available across sectors in cases of escalation – without mandatory "provisioning," but through agreed provision frameworks with compensation logic and incentive systems. Options include, among others:

→ availability contracts with sectoral performance classes (similar to AirTanker UK),

→ tax-subsidized redundancy structures in IT, energy, and logistics,

→ standardization of mobilization contracts through a federal framework,

→ integration of military requirements into emergency preparedness according to §8a BSIG for operators of critical infrastructures.

It is key that these models not only follow procurement logics, but also establish strategic partnerships, as envisaged by the British "Whole Force" concept or as the Finnish sectoral preparedness agreements achieve.

5.3 Platform for demand capacity balancing: digital integration layer for OPLAN DEU

A central deficit of the German security architecture lies in the lack of digital coupling between military planning and private sector capability. Based on the known principles of OPLAN DEU, the development of such a platform-based integration architecture is essential for its implementation. This is especially true for the creation of a common situation picture, but of course also for the control of tactical measures at the interface between the armed forces and the private sector.

Such a system should therefore map the following functions in a common, federally linkable structure:

→ survey of military planning needs (deployment axes, storage capacities, supply chains),

→ availability reporting of private sector capacities (IT, logistics, energy, personnel),

→ contract status management (service class, escalation level, rights/obligations),

→ real-time situation picture coupling (critical infrastructures, supply shortages, prioritization).

Such a system would be compatible with existing military command information systems and civilian situation maps (e.g., MoFIS, BBK situation center, state command staffs). International references exist in Finland (NESA situation picture integration) and in the United Kingdom (digital tasking systems with private sector contracting partners).

5.4 Building a strategic exercise culture: stabilization of operational coupling

The examples from Sweden (TFÖ 20), Finland (NESA crisis exercises), and the United Kingdom (STUFT deployment tests, AirTanker mobilization planning) show that comprehensive national defense capability cannot be maintained without continuous testing of institutional, technical, and logistical interfaces.

For Germany, this results in the need to establish an institutionalized training system that

→ synchronizes private sector–military situation representations,

→ practically tests resource reports and retrieval logics,

→ involves private sector actors in operational management processes through simulation,

→ regularly evaluates IT interfaces, communication protocols, and mobilization procedures.

Ideally, this system should be managed across different departments under the responsibility of the National Security Council (or NSR Situation Center), with annual focus exercises, sectoral stress scenarios, and the integration of international partner formats (e.g., NATO coordination, EU civil protection).

5.5 Integration of business: incentives, security, and legitimacy

The successful implementation of a digital platform for PMC significantly depends on the willingness of the private sector to contribute its resources and expertise. For companies to reliably participate in times of crisis, clear framework conditions are needed that create incentives, hedge risks, and ensure social legitimacy. With the order to the company Rheinmetall to set up Convoy Support Centers with a budget of 263 million euros[18], the Bundeswehr has made an initial, significant attempt at a stand-by contract. The Bundeswehr and companies have developed and applied methods to clearly define the results and create incentives for achieving them. This can serve as an example for further cooperations of this kind.

In general, the following applies: On the one hand, contractual and legal protection is key. Companies must be able to trust that their services are legally secured and that liability risks are clearly regulated. Without this security, there is a risk of reluctance, especially concerning critical infrastructure or security-relevant data. On the other hand, incentives are necessary that make engagement attractive in everyday life as well. This can be achieved through economic compensation mechanisms, crediting towards sustainability or CSR goals, as well as through the public visibility of the contribution.

[18] Rheinmetall AG: Rheinmetall gewinnt Auftrag zur logistischen Unterstützung der Streitkräfte, press release, February 19, 2025, online: https://www.rheinmetall.com/de/media/news-watch/news/2025/02/2025-02-19-rheinmetall-gewinnt-auftrag-zur-logistischen-unterstuetzung-der-streitkraefte (accessed October 28, 2025).

The crucial thing is that companies recognize the benefits of their involvement – not only in crisis mode, but also during the normal phase. Finally, socio-political legitimacy is required. Only when it is clear that private sector involvement is conducted in the public interest and based on clear rules does the acceptance necessary for a sustainable model arise. The state should develop binding incentive and safeguarding mechanisms while ensuring political and societal legitimacy through clear communication.

5.6 Summary and overview

The following overview summarizes the four key structural reform areas derived from the analysis of international best practices for the implementation of OPLAN DEU.

Field of Reform	Recommended Action	International Reference
National control	Development of an operational National Security Council (NSR) with a situation center in the Chancellery and vertical linkage to the states	Sweden (MSB)
Private sector integration	Introduction of sectoral readiness agreements with private sector service providers in critical infrastructure (KRITIS) areas	Finland (Preparedness Agreements, NESA)
Digital integration architecture	Development of a platform for coupling military needs with private sector capacities and situational pictures	United Kingdom (tasking systems), Finland
Exercise system and validation	Establishment of an institutional exercise framework for private sector–military resilience tests and resource mobilization	Sweden (TFÖ 20), UK (STUFT, AirTanker activation)

Table 4: Central structural fields of reform

5.7 Further research and action fields

This study primarily addresses the question of how established standards and best practices from the private sector can be utilized for the tasks of Operations Plan Germany. In doing so, it addresses an important, but by no means the only, field of action for a PMC. Defining and deploying this PMC is an essential requirement overall for realizing the desired defense capability.

One example is the creation of European solutions for the launch and operation of satellites. While private sector solutions like Starlink in the USA are able to launch satellites into orbit at around 20% of the European costs, the European system Ariane is currently not even able to launch. Here, too, a solution within the framework of a PMC is necessary and important.

6. Best Practices of Private Sector Logistics

Mechanisms that ensure resilience in industry provide blueprints for nationwide supply preparedness.

The previous analysis has shown which principles are central for the successful integration of the private sector into military contexts. While chapters 3 to 5 describe general, institutional, legal, and organizational prerequisites, this chapter focuses on the operational capabilities of the private sector itself. Many mechanisms that the private sector has developed for managing complex supply chains and global networks can be transferred to military logistics planning. This chapter therefore examines suitable best practices from the private sector that illustrate how the private sector effectively addresses existing logistical challenges and where cooperation potentials lie.

6.1 Initial situation and problem

The resilience of supply chains has become one of the central topics of private sector planning since the turn of the millennium. For decades, efficiency considerations dominated, particularly the focus on just-in-time (JIT) deliveries, lean inventory, and the most extensive possible international division of labor. This logic led to significant productivity gains, but at the same time made the global value chains vulnerable to disruptions. Individual events such as the COVID-19 pandemic, the blockade of the Suez Canal in 2021, and recent geopolitical tensions have demonstrated how quickly the failure of individual transport routes or suppliers can lead to massive disruptions. Global goods flows are so interdependent today that even short-term disruptions trigger significant cascading effects.

The private sector has learned from these experiences and has developed a number of mechanisms over the past years to make supply chains more robust. These mechanisms are not based on new theoretical concepts, but are the result of practical adaptations that have been successfully applied for years in various industries – from the automotive industry to manufacturing and even food supply. At the center are four principles:

→ the creation of transparency regarding supply chains in the form of digital situation reports,

→ proactive planning through simulation and scenarios,

→ the combination of just-in-time approaches with targeted buffer stocks, and

→ contractual safeguarding and escalation capability in relation to suppliers.

6.2 Transparency and digital situation overview

One of the central lessons from the crises of recent years is that resilience cannot be achieved without transparency. Companies need to have an overview of inventories, transportation flows, and available capacities at all times – not only in their own facilities, but throughout the entire value chain. In the private sector, what are known as Supply Chain Control Towers have been established for this purpose. These systems aggregate data from a wide variety of sources, from Enterprise Resource Planning (ERP) systems to transport management, warehouse management and external information on topics such as traffic or weather, and consolidate it into a real-time situational picture[19]. The benefit of such a situation report is not only making the status quo visible. It also makes it possible to detect deviations early and

[19] McKinsey & Company: Supply chains to build resilience, manage proactively, online: https://www.mckinsey.com/capabilities/operations/our-insights/supply-chains-to-build-resilience-manage-proactively (accessed October 28, 2025).

to take targeted countermeasures. If, for example, a delayed delivery is likely, transport chains can be rerouted, alternative suppliers activated, or intermediate storage used before production comes to a standstill. Modern control tower systems are not only passive observers, but also have automated early warning mechanisms that immediately raise an alarm and initiate escalation processes in the event of critical deviations.

Another development that is gaining increasing importance is the use of what are known as digital twins. The entire supply chain is virtually mapped and fed with operational data in real time. The digital twin not only makes existing processes transparent, but also allows for the simulation of future developments. In this way, companies can calculate the impacts of disruptions, as well as demand spikes or geopolitical influences, in advance, and prepare appropriate courses of action[20]. This makes transparency not just a reactive observation, but a proactive management tool.

6.3 Scenario planning and simulation

Resilient supply chains are characterized by not only responding to current disruptions, but also anticipating potential crises in advance. In private sector practice, it has therefore become common to play through scenarios ranging from the failure of individual suppliers or the collapse of transport routes to sudden demand shocks. The aim of these plans is to avoid having to improvise in an emergency, but rather to be able to fall back on prepared alternatives.

Digital twins and control towers provide the technical foundations for this. They allow "what-if" analyses, in which various disruptions are simulated and the impacts on the entire value chain are made visible. This way, stress-tested supply chains are created that already have alternative sources, alternative routes, or additional buffers in advance. This practice has proven effective as a digital process twin, enabling continuous risk assessment and the implementation of countermeasures in the system. Digital twins are predestined to combine transparency with simulation-based emergency plans[21].

This makes scenario planning an integral part of private sector resilience architecture: It creates the ability to quickly respond to unforeseen events because the corresponding options have already been designed, tested, and organizationally prepared.

6.4 Hybrid inventory strategies

A third principle concerns the question of how efficiency and resilience can be harmonized. Pure just-in-time logistics does minimize storage costs, but it has proven to be highly susceptible to disruptions. Pure stockpiling, on the other hand, increases robustness but ties up capital and space. In private sector practice, a hybrid model has therefore become established. Non-critical parts continue to be procured according to JIT logic, while critical components with a high risk of failure or long lead times are specifically stocked.

[20] Roman, D.; Schneider, M.; et al.: Digital Twins for Supply Chain Simulation: Methods and Applications. In: Logistics 2025, 9(1), 22, online: https://doi.org/10.3390/logistics9010022 (accessed October 28, 2025).

[21] MHP Management- und IT-Beratung GmbH: Digitale Zwillinge – Neue Perspektiven für Lieferketten, white paper, March 2024, online: https://www.mhp.com/fileadmin/www.mhp.com/downloads/whitepaper/MHPWhitePaper_DigitalTwins_DE.pdf (accessed October 28, 2025).

The BME Logistics Study 2024 shows that over 80% of the surveyed companies have increased their inventories since the pandemic to ensure supply security[22]. This shows that risk-adequate segmentation of goods is crucial: Inventories are built up where a failure would have particularly serious consequences, while lean processes continue to apply in stable areas[23].

This principle allows efficiency and resilience to be viewed not as opposites, but as complementary objectives. The targeted combination creates a supply system that remains cost-efficient while still possessing the necessary robustness to withstand disruptions.

6.5 Supplier management and escalation

In addition to technology and inventories, structuring relationships with suppliers is a central component of resilient supply chains. In many industries – especially in the automotive industry – service level agreements are established that definitively set quality requirements, delivery times, and response processes.

In addition, multi-level escalation mechanisms have been established. If deviations from the agreed standards occur, early warning messages are initially triggered, followed by graduated action plans, and in extreme cases, the substitution of the supplier. This escalation logic ensures that risks become visible at an early stage and do not only come into effect in a crisis. It enables a partnership-based, yet binding relationship between companies and suppliers[24].

6.6 Classification in the context of OPLAN DEU

The presented best practices show that resilience is not a theoretical construct, but a lived private sector practice. Companies have proven over the years that supply chains can be made more resilient through transparency, scenarios, buffers, and contracts.

For Germany as a logistical hub in the NATO context, clear points of connection arise from this. Transparency in the form of digital situational pictures directly corresponds to the necessity to create a nationwide supply situation picture for host nation support. Scenario planning and simulation can be applied to the preparation of troop deployments and supply operations. Hybrid inventory strategies should be considered analogously with regard to critical resources such as fuel, accommodation capacities, or means of transport. Contract management and escalation logic ultimately corresponds to the necessity of being able to reliably activate private sector services in the event of a crisis.

[22] Bundesverband Materialwirtschaft, Einkauf und Logistik e. V. (BME): BME-Logistikstudie 2024 – Risikomanagement und Resilienz in Supply Chains, Eschborn 2024, online: https://www.bme.de/fachinformationen/bme-logistikstudie-2024/ (accessed October 28, 2025).

[23] Siemens AG; Frost & Sullivan: Building Sustainable and Agile Industrial Supply Chain, Munich, 2021, online: https://assets.new.siemens.com/siemens/assets/api/uuid:a63fafc9-5d55-48ba-89e7-5d58c4bfb87d/Building-sustainable-agile-industrial-supply-chain-Frost-Sullivan-original.pdf (accessed October 28, 2025).

[24] German Association of the Automotive Industry (VDA): Basic principles of collaboration between automobile manufacturers and their partners, 2022, online: https://www.vda.de/dam/jcr:b531a4a2-8873-4c84-8bd2-78ebd3078862/VDA_5867_Principles_for_the_Management_Board_HG_III_RZ2.pdf (accessed October 28, 2025).

7. Example Solution Proposal: German Digital Supply Hub

The Digital Supply Hub is not an IT project, but a strategic tool for linking public responsibility and needs with private sector capabilities.

As presented in Chapter 2, OPLAN DEU is an operationally oriented command plan of the Bundeswehr, which, as far as is known, coordinates military deployability, command structures, and logistical operations within the framework of national and alliance defense. As a NATO member, Germany acts as a logistical hub for allied forces.

While OPLAN DEU is a military concept, there are currently no sufficient structures to systematically integrate civilian and particularly private sector resources. It is undisputed that the Bundeswehr would not be able to manage large-scale troop movements, material handling, or allied supply hubs on its own in the event of tension or crisis. The operational effectiveness significantly depends on the support from federal departments, states, and the private sector – particularly in the areas of transport, energy, communication, accommodation, and emergency logistics.

International best practices (see Chapter 4) show that integration of the private sector can succeed if it is structurally prepared: The Netherlands secures its role as a logistical hub through public–private agreements led by the National Coordinator for Counterterrorism and Security (NCTV). Finland controls private sector resources through sectoral readiness contracts under the umbrella of the National Emergency Supply Agency (NESA). Sweden relies on a federally coordinated network of authorities, businesses, and military stakeholders. The United Kingdom integrates private sector capabilities directly into operational logic through contractually regulated tasking systems. What these models have in common is that their effectiveness depends on the presence of a common situational awareness of private sector resources.

In Germany, however, there is still no common, systematic overview of privately usable supply resources that can be systematically aligned with military needs. Military systems and structures so far do not allow the integration of private sector services. Private sector systems, such as large operators' ERP systems, are again not interoperable, are proprietary in their operation, and have neither federal connectivity nor mechanisms for nationwide coordination in defense situations. The Bundeswehr's TerrHub approach also primarily focuses on governmental infrastructures and is not designed for private sector cooperation structures.[25]

The existing systems are therefore valuable subcomponents, but they are structurally unable to bridge the gap between military demand logic and private sector supply. A proprietary further development of individual platforms or systems cannot remedy this deficit; instead, it would undermine the claim of equal resilience partnerships. What is needed, rather, is an open, modular, and connectable capability framework that complements existing systems in an interoperable manner while also being independently controllable.

The aim of the concept is to make the alignment between military needs and private sector capacities digitally controllable – through transparent data models, interactive decision aids, and scenario-based planning functions. The basis would be real-time data from the German private sector, which can be integrated through framework agreements. Military data itself would not be part of the platform; its sovereignty would remain entirely with the Bundeswehr. However, the architecture would be designed in such a way that

[25] BMVg: Wehrwissenschaftliche Forschung – Jahresbericht 2024, online: https://www.bmvg.de/resource/blob/6001656/8b2973bb7908f6e09e0dd3bd1ed1e827/wehrwissenschaftliche-forschung-data.pdf (accessed October 28, 2025).

a technical integration of military data would be possible if needed, without abandoning the clear separation of responsibilities.

Three core functions are at the center of this:

1. Transparency:

Making relevant civilian or private sector resources, infrastructure nodes, and services visible;

2. Connectivity:

Coordinated mapping of demand carriers, resource providers, and supportable actors;

3. Predictability:

Scenario-based validation, prioritization, and activation logic for support measures – from the supply of fuel and fleet capacities to logistical services and the temporary use of private sector areas.

A significant advantage of the platform would be the ability to generate a consolidated real-time situational picture of the nationwide usable supply capacities based on the data of an infrastructure twin and a service twin. The AI-supported logic would not only evaluate potential Convoy Support Centers (CSC), but also private sector capacities in areas such as transportation, energy, workshop infrastructure, or emergency logistics. This would create an adaptive supply situation picture that makes bottlenecks transparent, prioritizes available resources, and is strategically, operationally, and tactically usable both in peacetime and in crisis and defense situations.

Users could interactively evaluate such a situation report, identify supply gaps, and activate capacities in a targeted manner. This could include, for example, the provision of diesel by a refinery, the allocation of transport fleets, or the use of private business premises as temporary supply locations. This would create a digital decision space in which military needs and private sector capacities can be proactively synchronized – without operational disclosure, but with real planning ability.

The German Digital Supply Hub could be divided into three coordinated modules:

Module 1 – Infrastructure twin:

Digital recording and assessment of relevant infrastructures and logistical hubs according to system-critical criteria for supply and mobility. Example content: tank storage, truck parking areas, rail terminals, port handling areas, large parking lots, access roads.

Module 2 – Service twin:

Overview of logistics-related services and private sector support services with standby and activation logic.

Example content: freight forwarding services, emergency power generators, sanitary container services, catering services, mobile communication units and contractually guaranteed fleet capacities, diesel stocks from refineries or private commercial workshops

Module 3 – Supply situation dashboard & simulation:

Scenario-based planning support for decision preparation as well as the visualization of aggregated demand and supply situations. Example: matching of available transport and energy capacities, logistical services and space options for the short-term creation of supply hubs

The illustration on page 48 visualizes the interaction of the three modules within the framework of private sector–military supply coupling and overall state supply transparency.

7.2 Dimensions of the Digital Supply Hub: strategic, operational, tactical

The German Digital Supply Hub would be more than a technical tool. Its impact and benefits would manifest at all levels of security policy action – strategic, operational, and tactical. The core of the Digital Supply Hub lies in the consistent integration of private sector supply capacities, which have not yet been systematically integrated into nationwide planning. Military data is not part of the platform; at the same time, its architecture is designed in such a way that no conclusions can be drawn about military projects or operations. This would create an instrument that enables precautionary measures in peacetime, ensures coordination in times of tension, and can provide a reliable basis for activating private sector services in defense or Article 5 scenarios.

7.2.1 Strategic level

The strategic significance of the German Digital Supply Hub would lie in its ability to systematically integrate private sector data and capacities into the national contingency planning. It would not only enable the implementation of existing concepts, but also lay the foundation for developing and continuously adapting a coherent national supply strategy. By integrating private sector data, it would make visible which resources are actually available, where structural bottlenecks arise, and which capacities must be secured in the long term. This would create a fact-based decision-making foundation to identify strategic capability gaps and to allocate budget resources precisely where they will have the greatest impact on resilience.

The scenario-based simulation functions could develop the Digital Supply Hub into a strategic testing ground, allowing different strategic development scenarios to be played out based on private sector capacity reports, such as the effects of large-scale energy shortages, critical dependencies, or long-term availability risks. Strategic decision-makers would thus not only gain transparency, but also concrete options for further developing the national supply strategy.

In defense or Article 5 scenarios, the platform could ultimately reach its maximum effectiveness by enabling the targeted prioritization of private sector capacities in an aggregated form and making them plannable over longer periods. It would answer the crucial questions: What private sector resources are actually available, how long can they last under what conditions, and what needs must be secured in advance? This would stop preventive measures

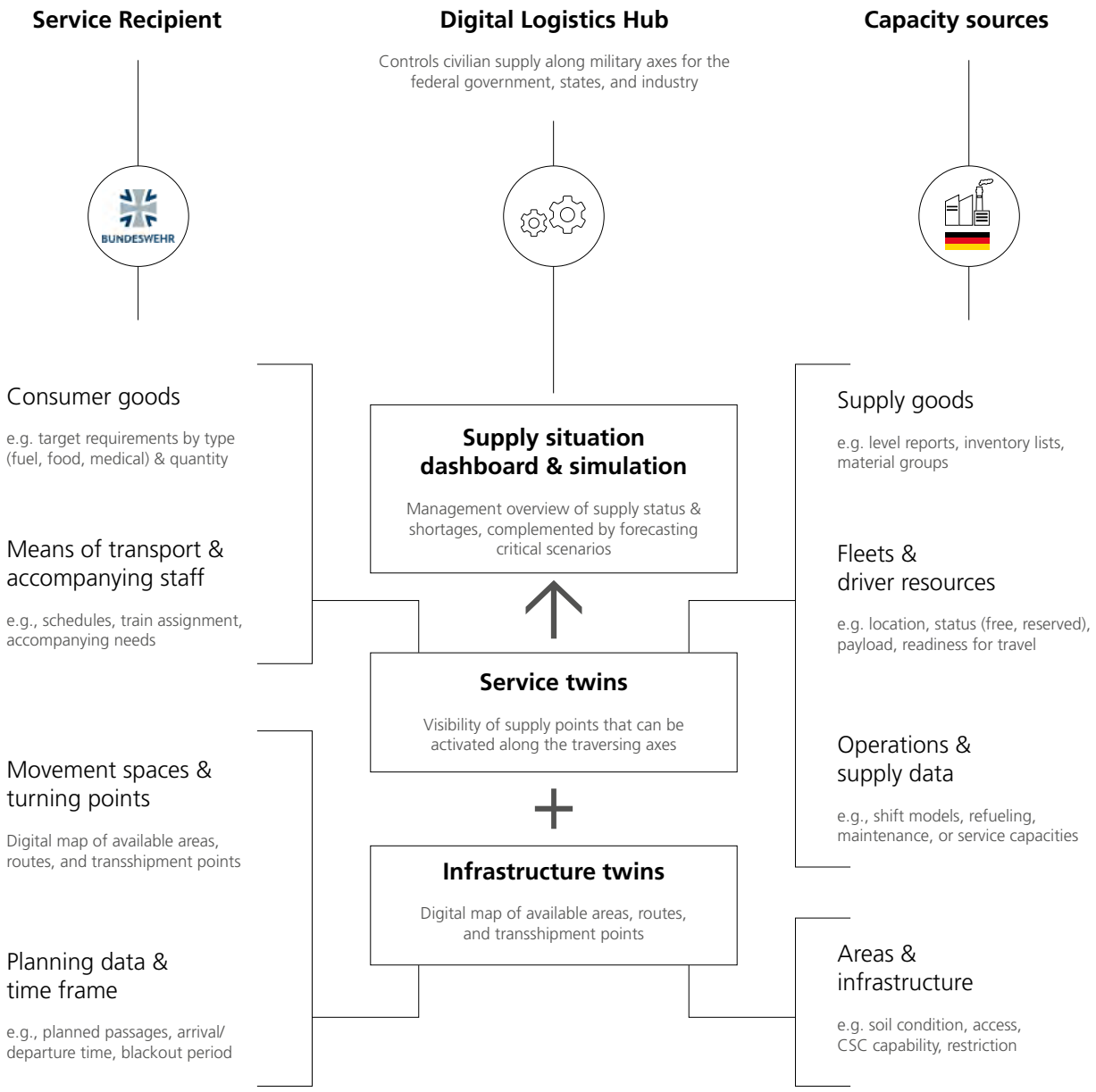


Figure 2: Interaction of the three modules

from remaining in place in the form of blanket availability commitments. Instead, a reliable basis would be created to specifically integrate private sector services into Germany's resilience, and sustainably secure its role as an alliance logistical hub.

A potential user group and information recipient of the strategic level of the Digital Supply Hub could be the German Federal Ministry of Defence (BMVg). In this case, the main department would be Armed Forces (SK); SK II Support Tasks and Logistics would be conceivable. The ministry could also bring the available information into the interministerial coordination and the parliament to justify, for example, budgetary funds.

7.2.2 Operational level

The operational level of the Digital Supply Hub would be based on the ability to merge needs and available capacities in real time into a consistent supply situation overview and to derive immediately actionable control decisions from it. While the strategic level would enable long-term planning and prioritization, operational use would consistently focus on ensuring ongoing operations and their flexible adaptation to changing situations.

In times of peace, the platform would serve practical preparation: Processes could be practiced in a realistic manner, alert routes tested, and collaboration with private sector partners concretely tried out. This would not only check which resources are available, but also whether their activation works reliably in case of need. In phases of increased tension, the platform would form the basis for operational control decisions.

It would enable the coordinated activation of resources, the prioritization of locations, and the short-term establishment of additional supply focal points. Transport routes could also be flexibly redirected or overloaded nodes could be relieved. In defense or Article 5 scenarios, the operational dimension would ultimately ensure the real-time synchronization of private sector capacities. Bottlenecks would be forecast early and backed with alternative options. Supply operations, such as fuel deliveries or the provision of fleet capacities, could be triggered immediately and tracked seamlessly. Decisions would thus not be based on estimates, but on an up-to-date, private sector data basis that would enable reliable operational control without revealing military leadership information. Possible user groups would be the Operational Command or the Logistics Commands, which could fulfill their operational responsibilities and pursue the implementation of strategic guidelines based on real-time data. At the same time, operational actors could use the information they receive from the tactical level to incorporate it, along with their own information, into the advisory process at the strategic level.

7.2.3 Tactical level

At the tactical level, the Digital Supply Hub would be effective in immediate execution and supply on-site: While the operational level could control and prioritize resource flows, the tactical dimension would provide a concrete decision-making basis for units and logistical entities in action. What would be crucial here are not long-term plans, but rather reliable information about which private sector resources are actually available at a specific location, under what conditions they can be used, and within what time frame they will be provided.

In times of peace, the platform would enable realistic preparation through exercises in which private sector resources were actually integrated. For example, troops could test how refueling from an external refinery, providing mobile catering, or using privately used areas as temporary gathering points would work in practice. In phases of increased tension, the platform would become an immediate tool for responsiveness. Gaps in supply could be directly closed, convoy support centers could be set up at short notice, and locally available capacities could be specifically activated. This would strengthen the ability to respond to dynamic situations without delay.

In the event of defense requirements or an Article 5 scenario, the Digital Supply Hub would directly support the deployment operations. It would ensure that logistical units are not reliant on assumptions, but have access to up-to-date and reliable information, whether for the immediate provision of fuel, the allocation of transport fleets, or the use of privately operated sites. The platform would not replace military leadership, but would enhance tactical capability by securing decisions through precise, privately sourced data.

A potential user group and information recipient of the tactical level of the Digital Supply Hub could be troop units on the move or on-site, as well as logistics units of the active troops or the reserve.

Summary

A German Digital Supply Hub could be effective on three levels:

→ At the strategic level, it would provide an initial factual basis to integrate private sector data into national contingency planning. It would make capability gaps visible, enable simulations as a strategic laboratory, and direct budget decisions specifically to critical demand areas. This would make prevention not abstract, but measurable, verifiable, and continuously adaptable.

→ At the operational level, the platform would be used to manage ongoing processes. Needs and capacities would be combined in a consistent situational picture, allowing resources to be prioritized, supply focal points to be established, and transport axes to be flexibly adjusted. The real-time synchronization of private sector capacities would prevent processes from stalling, ensuring that supply remains continuously manageable.

→ Finally, at the tactical level, the Digital Supply Hub would support the immediate execution on-site. It would provide troop units and logistical units with precise information on the availability, conditions, and time frames of private sector resources. This would ensure reliable provision – from fuel supply to the use of private commercial areas – without replacing military command structures.

Private sector data would be the connective core at all levels: It makes strategic planning robust, operational control reliable, and tactical execution immediately actionable. The Digital Supply Hub could thus become the crucial link that enables Germany not only to describe its role as a logistical hub in the an alliance, but to implement it practically and permanently.

7.3 Infrastructure twin: digital topography of supply capacities usable nationwide

The infrastructure twin would form the structural foundation of the German Digital Supply Hub. The objective would be to establish a digitally usable, up-to-date, and assessable representation of infrastructural and private sector resources that would be significant in the context of national crisis preparedness as well as private sector provisioning capacities. Unlike a military situational picture, the infrastructure twin would not generate operational command information. Rather, it would serve as a data-based framework for the private military amalgamation of needs and potential usage possibilities.

The module could capture and evaluate both public and private sector infrastructures, whose location, condition, and usability could be relevant for logistical support tasks in crisis or defense situations. This includes, among other things, truck rest areas, tank storage, loading yards, factory access roads, rail loading points, large parking lots, as well as temporarily usable areas in industrial zones. Bridge loads, rail networks, river crossings, or private business premises that are made available for logistical purposes could also be recorded.

The data basis could be sourced from existing administrative records, geographic information systems, and critical infrastructure registers, but would be significantly expanded by proprietary data from the private sector – particularly from the logistics, automotive, and manufacturing sectors.

Proven use in the private sector

In private sector practice, two principles have been established that can be directly applied to the infrastructure twin: transparency through digital situation reports and proactive scenario planning.

Companies use what are known as Control Towers for this purpose, which consolidate data on transport routes, transshipment points, and failure reports into a consolidated real-time view. Deviations – such as blocked access roads or reduced capacities – are not only visible in the event of an incident, but are detected early and automatically backed up with options for action. Similarly, digital twins in the private sector use simulations to anticipate the failure of individual nodes or routes and to provide alternative pathways.

The infrastructure twin would adopt this logic by transforming roads, bridges, railway terminals, tank storage, and other nodes into a consolidated, dynamically updatable situation overview. Instead of abstract transparency, this would create a concrete overview of infrastructure usable throughout the entire state, making constraints (e.g., closures, construction conditions, flood levels) directly visible and suggesting alternative corridors.

This would transfer the private sector principle of transparency to the security policy context: not as production assurance, but as a method of securing critical supply routes in the event of an alliance situation. Additionally, the infrastructure twin would take on the role of scenario planning by simulating how the failure of individual bridges, road sections, or railway crossings affects overall logistics – and which alternatives can be activated.

This would create a practically usable translation of private sector best practices: The infrastructure twin is not a passive register of areas, but an active instrument that combines transparency and simulation, thereby making the core contribution to nationwide supply security.

7.4 Service twin: multidimensional visibility of private sector supply chains

The service twin would complement the infrastructure twin with the dimensional level of available services. While the infrastructure twin could classify physical locations and areas, the service twin would describe the deployable functions and capacities that could be available at these locations or in their surroundings in the event of defense or crisis scenarios. This module would not replace an operational situation picture either, but would instead structure and dynamically represent those private sector support services necessary for the supply, care, assurance, or transit of military forces and civilian stakeholders.

The focus of the module would be on the digital recording, categorization, and qualified description of available services, including quantity information, response times, activation conditions, quality features, and, if applicable, restrictive conditions. The recorded services would range from transport, storage, and catering services to sanitary facilities, mobile energy supply, and water supply and disposal, as well as temporarily available communication and security services. Even specialized services such as lifting technology, mobile data centers, basic medical care, or emergency shelter systems could be covered, provided they are mobile and can be integrated contractually.

An essential feature of the service twin would be the ability not only to manage master data about providers and service categories, but also to integrate current availabilities, utilization levels, and call-off deadlines. This could be done either through standardized interfaces (e.g., API-supported capacity messages) or through a central maintenance infrastructure. The aim would not be real-time daily tracking, but rather an appropriate, reliable assessment of available support options – for instance, the provision of transport fleets, fuel or workshop services, or the temporary establishment of a logistical transshipment corridor.

Proven use in the private sector

In private sector practice, two principles in particular are established that can be directly transferred to the service twin: hybrid inventory strategies and supplier management with escalation logic.

Companies specifically rely on buffer stocks for critical resources – such as special parts or energy-intensive materials – while non-critical

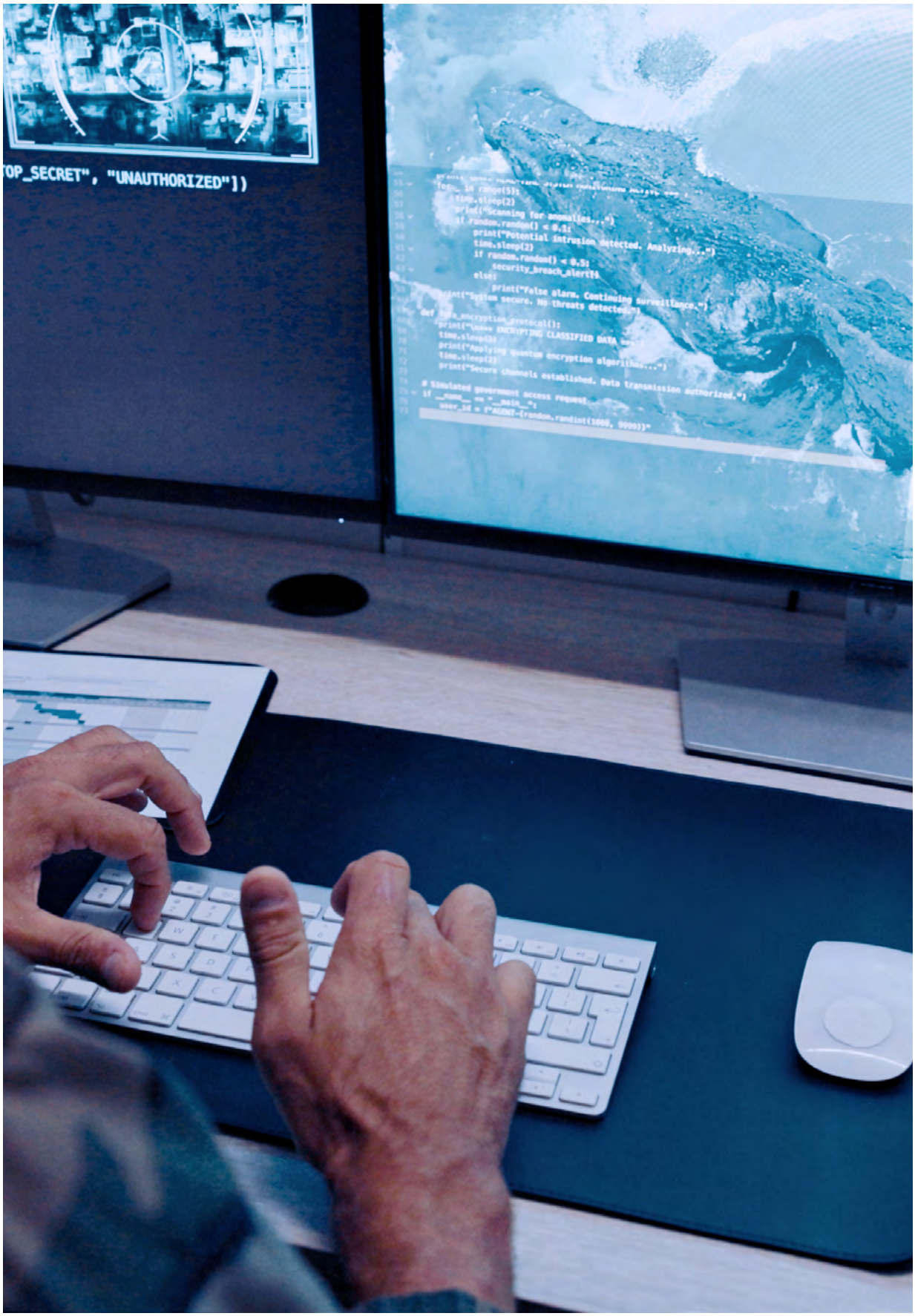
services continue to be provided according to the just-in-time logic. At the same time, services are contractually regulated through service-level agreements (SLAs): Delivery times, quantities, quality standards, and escalation levels are established in binding form. If deviations occur, graduated escalation processes are triggered, ranging from early warning notifications to the substitution of the service provider.

The service twin would transfer this logic into the security policy context. It would not only capture the type of available services – such as transport fleets, diesel supplies, workshops, or emergency power generators – but also their contractual activation conditions, response times, and escalation paths. Instead of a mere overview, a robust image of essential supply services would thus be created, which would be reliably available and retrievable in the event of a crisis. Particularly relevant would be the depiction of hybrid strategies: Critical resources such as fuel or healthcare would be managed in the system as stored and available for quick activation, while other services (e.g., catering or mobile sanitary systems) would be flexibly integrated as needed. This would cause the service twin to reflect exactly that graduated resilience logic that companies have been using for years to keep supply chains stable.

This is how a practical transfer of private sector best practices is put in place: The service twin is not a static list of services, but a dynamic instrument that integrates contract logic, inventory management, and escalation mechanisms – thereby enhancing the overall state ability to make private sector services quickly and reliably available in the event of a defense scenario.

7.5 Supply situation dashboard & simulation: controllable through a jointly shared reality

The Supply situation dashboard & simulation module could form the decisive functional component for the multidimensional utilization of the Digital Supply Hub. It would transform the data stored in the infrastructure and service twin into an interactive, usage-oriented overview of the national supply situation within the framework of national and alliance defense. Unlike a military situational picture, this module would not be geared towards tactical leadership, but rather towards the coordination and proactive management of support services along logistical deployment axes, with a particular focus on Germany's role as a logistical hub for NATO forces. The central challenge is that there is currently no cross-organizational overview that brings together military support needs and private sector capacities in a dynamic, decision-relevant format. Especially in the context of strategic marching routes, there is a lack of a transparent, real-time representation of private sector resources – such as fuel, parking spaces, sanitary facilities, or workshop services – and clarity on how quickly these could be activated. Questions about suitable transport corridors, energy and fuel capacities, workshop and storage infrastructures, or municipal areas also remain open. In all cases, it is necessary to clarify: Which locations are suitable at all? Which modules (e.g., catering, sanitation, energy) are available at which location? Who is the operator? Which services can be activated within what time frame – and on what basis?


OP_SECRET", "UNAUTHORIZED"])

The supply situation dashboard could address this structural gap. It would connect the digital twin models with an intuitive, role-based interface where supply options, current capacities, and demand developments are consolidated. This would create an interorganizational decision-making space that would be federally compatible and capable of being synchronized between the private sector and the military – without taking on operational leadership responsibility.

A central element would be an interactive supply map that displays all potential support locations and activated supply facilities on an interactive map of Germany. This representation could be supplemented by regional supply profiles, a configurable "resource heatmap," status messages on operational restrictions, and digital fact sheets for each location. For prioritized supply points, whether transport hubs, energy capacities, or potential CSCs, a dedicated operations monitor could be called upon to aggregate critical parameters such as energy availability, medical status, delivery priorities, or module utilization.

A particularly effective use case would be the ability to interactively simulate different supply scenarios – such as the short-term establishment of additional supply focal points, the stabilization of transport chains, or the temporary activation of private sector capacities. Users would select possible CSCs on the map for this purpose. The system could show the following information for each point:

→ the availability status (available, limited, not usable),

→ the current supply situation (e.g., diesel level, parking area, sanitary unit),

→ reaction times, and

→ the underlying contractual activation logic.

If a location is marked as restricted (e.g., diesel is lacking), supply could be ordered with a click, based on the contract data stored in the system. This includes not only the performance class, quantities, prices, and responsibilities, but also agreed response times and escalation mechanisms. The supply process (e.g., 10,000 liters of diesel in 24 hours from the contracting partner Shell) would be directly initiated in the dashboard, made visible, and automatically updated after successful execution. The status could subsequently change to "Supply active" – thereby transforming the dashboard from a situational overview to an operational tool.

Simulation capability as a central element

An integral component would be scenario-based simulation. Building on the twin data, the system would enable the forecasting of stress situations along the hub axes – for example when several NATO units land simultaneously, a location fails, or there is a temporary shortage of services. AI-based algorithms could identify bottlenecks, alternative routes, or necessary pre-shiftings at an early stage. This function could support not only operational planning bodies, but also federal decision-making levels and private sector actors in the forward-looking fine-tuning of logistical relief points, for example by preparing alternative CSCs or temporarily expanding supply capacities.

The need for such an instrument arises not least from reality: Germany currently lacks a nationwide,

private sector–military integrated overview of available supply capacities. The flow of information is sectorally fragmented, static, and reactive – instead of dynamic and open to coordination. Organizations such as Autobahn GmbH, the rail network, state authorities, infrastructure providers, and military demand signalers often operate on separate databases – without binding control options.

By intersecting available areas with supply potentials, ownership structures, infrastructure conditions, and contractual activation logics, a reliable data basis for algorithmic evaluations would be created with the dashboard and the twins. This database could be used to identify, prioritize, and provide suitable locations and capacities for scenario-based planning – without disclosing military routes. The evaluation would be based on understandable criteria (e.g., logistical accessibility, supply security, capacity for activation) and enable an appropriate pre-selection for contractual security, exercise integration, or preliminary negotiations with owners.

The AI logic would not be limited to static infrastructure properties, but would take dynamic situational changes – such as closures, usage conflicts, or updated supply situations – into account and integrate them into the assessment. This would create an adaptive CSC proposal image that could be continuously adjusted and that would provide realistic decision-making bases for political, administrative, and military stakeholders.

Proven use in the private sector

The supply situation dashboard consistently applies the previously described private sector best practices to the security policy context. The transparency proven in the control tower approach is used to make the current supply situation – such as available CSC, tank storage, or transport capacities – visible in a consolidated form.

The logic of private sector scenario planning is reflected in the simulation-supported functions: Users could simulate how the situation changes when a location fails, additional troops need to be rerouted, or resources become scarce at a given point. The system would then display prepared alternative options, prioritize available resources, and mark which actions could be activated immediately. The AI-supported forecasts established in the private sector would also be adapted. Algorithms would analyze historical patterns, current malfunction reports, and contract data to identify bottlenecks in advance and suggest specific actions, such as rerouting or additional capacities.

This turns the dashboard into an active decision tool that combines transparency, simulation, and AI-supported forecasts in an adaptive supply situation overview. It is not an additional level of management, but rather a connecting instrument for situational awareness and control, synchronizing military needs, federal responsibilities, and private sector capabilities on a common platform. Especially in situations where supply decisions are required at short notice, it enables robust, evidence-based decision-making – thus creating the operational prerequisite for Germany to actually fulfill its role as a logistical hub within the framework of its alliance commitments.

7.6 Interface and data integration

The German Digital Supply Hub would be based on the structured consolidation of data from different source systems. This integration would require a bindingly defined interface logic that ensures both technically and organizationally that information about available infrastructures, private sector support services, contractual situations, and regional supply capacities can be systematically incorporated, kept up to date, and used in a targeted manner – without interfering with operational management processes or compromising security-critical information. Data from the Bundeswehr would remain exclusively in military systems; it would not be transferred to the hub. This would mean that the platform would fundamentally operate in the unclassified area, with data security and confidentiality guaranteed at all times.

The goal would not be to establish a central database, but rather a distributed, federated data exchange framework. This could utilize existing systems, rely on standardized exchange formats, and take into account clearly defined roles and responsibilities. The technical architecture would follow the following logic: What matters is not where data resides, but who contributes or retrieves it when, at what depth, and with what liability. A differentiated rights and roles concept would ensure that the platform could be used at tactical, operational, and strategic levels – by military end users, government agencies, as well as state and local authorities, each with graduated information access.

The benefit of the platform is only fully realized when the individual modules can access a reliable, regularly updated database:

→ The infrastructure twin requires information about the location, condition, ownership, and usability of physical areas.

→ The service twin requires structured performance data on private sector support services, including response times and activation paths.

→ The supply situation dashboard can only be effective if standardized feedback from federal, private, and operational systems regarding restrictions, operational changes, bottlenecks, or contract-based supply triggers is provided.

This would require a multi-layered interface architecture that covers the following dimensions:

1. Institutional affiliation

Integration of all relevant data providers – from federal agencies to municipal authorities and private sector service providers – into a binding, controllable governance structure. Each partner knows their data contribution, the reporting frequency, the response logic in the event of an incident, and the quality assurance obligations.

2. Technical connectivity

Use of proven exchange formats (e.g., CSV, XML, REST APIs), as used in comparable government platforms – for example in the ATLAS customs system, the European EESSI procedure, or the market master data register. The use of proprietary software solutions is not intended; rather, an open, modular approach should enable broad connectivity.

3. Security and access protection

The platform fundamentally operates in the unclassified domain. Sensitive or classified data remains entirely within the military specialized systems. The rights and roles concept ensures that only authorized actors have access to exactly the types of data and functions that correspond to their respective level – such as contract data, operator assignments, or service agreements – with graduated permissions.

4. Dynamic content

The interface not only supports the provision of static master data (e.g., Tank Storage XY – 10,000 m^2, municipally owned), but also dynamic operational information such as:

→ temporary closures or restrictions,

→ live capacity reports,

→ information on existing supply contracts (including retrievable supply orders and conditions, e.g., diesel supply by third-party service providers),

→ failure or escalation notifications.

This real-time or near-real-time data is a central requirement for the activatable controllability of the supply chain – for instance, when specifically building a CSC or relieving a planned supply corridor.

Summary

The Digital Supply Hub is not an IT project, but a strategic tool for linking public responsibility and needs with private sector capabilities. It aims to close the structural coordination gap that currently prevents military needs, federal responsibilities, and private sector resources from working together in a crisis. With reference to Chapter 6, it also becomes clear: The proposed German Digital Hub does not rely on abstract concepts, but systematically transfers proven private sector mechanisms into the security policy context.

The key is that this model is not conceived as an isolated federal project, but as a nationwide collective task – as Team Germany comprising administration, business, strategic infrastructure operators, and operational service providers. The future viability of Germany's alliance capability does not depend solely on equipment and leadership – but on whether it succeeds in rethinking supply in an integrable, visible, and cooperative way.

8. Conclusion and Outlook: Summary of the Key Findings and Recommendations for Action

Defense capability does not arise through new institutions, but through functionally networked actors: the state, business, and society as a joint system.

The present study uses the framework of Comprehensive Defense as a conceptual reference to functionally integrate PMC into the national security architecture. The framework describes how defense capability arises from the interplay of several segments – from military defense to economic defense and social defense – and how crucial it is to consider interactions and relationships in a holistic view. The results of this study flesh out this approach using the example of the military defense segment: They show how private sector resources can be effectively incorporated into a functionally integrated architecture. This may also lead to conclusions about other segments that would need to be examined in more detail in further studies. Further or related questions could be: How can the performance and resilience of the private sector service providers who make concrete contributions to the implementation of the German hub be secured within the framework of economic defense? In the area of social defense, how effective and resilient cooperation between the private sector and emergency services can succeed could be examined. The goal could be to develop a plan analogous to OPLAN DEU for emergency services.

In the field of military defense, the implementation of OPLAN DEU is significantly dependent on the availability, visibility, and ability to activate private sector resources. These are assumed in OPLAN DEU. This requires an appropriate framework, which takes into account all technical, legal, and military requirements while benefiting from the best practices of other nations and the private sector.

This, in turn, needs a nationwide integration architecture that brings together public, federal, and private sector actors – structurally, procedurally, and digitally. In terms of the Comprehensive Defense Framework, however, this does not mean a new institutional hierarchy, but the functional linking of existing responsibilities.

The German Digital Supply Hub outlined in this study meets these requirements. The modular, open-interface platform solution does not replace military command systems, but creates a complementary supply situation overview – focusing on infrastructures, services, and usage potentials. It exemplifies the functional integration of central transparency (situation picture) and decentralized implementation competence (departmental and regional responsibilities) within a comprehensive national security understanding.

In addition, it is based on information as it is already made available by companies to each other in today's business relationships. In the event of an incident, it ensures that private sector service providers can be proactive, prepared, and coordinated. The aim and benefit do not lie in centralist control, but in reliable, real-time data-based coordination across institutional and sectoral boundaries.

To implement such a solution, a number of prerequisites must be established:

1. Political-administrative anchoring and open private sector architecture

Solutions like the German Digital Supply Hub require sponsorship with a nationwide perspective. The National Security Council and the proposed National Situation Center in the Federal Chancellery could serve as an integration platform that brings together information, needs, and priorities from the federal government, states, business, and armed forces. An open, modular architecture without proprietary hurdles is a fundamental requirement for broad connectivity in the federal, and especially in the corporate, environment. In addition, it creates conditions for integrating all the important information for situation assessment and task prioritization – the aforementioned functional integration that is necessary not only for PMC, but for all national security preparedness tasks.

2. Development of a sector-specific data and provision framework for private sector partners

Private sector partners have supply-relevant data that has not yet been systematically recorded or made available, such as information on land availability, transport capacities, transshipment points, reaction times, or service reserves. Clearly defined, legally viable models are needed for the voluntary or contractually regulated provision of this information – while maintaining data sovereignty, confidentiality, and competitive neutrality. Fundamentally, the proposed exchange is already established business practice.

3. Creation of material and immaterial incentives for private sector involvement

The integration of the private sector can only succeed if the state provides reliable incentive structures. These include: access to government emergency formats, institutional visibility, avoidance of redundant data requirements, documentable contribution to the resilience strategy, and a partnership role in strategic supply security. The participation must be economically reasonable and politically appreciated. With the order for Rheinmetall to set up Convoy Support Centers and the integration into the exercises of the armed forces, the Bundeswehr is testing a solution for such tasks. Cooperations of this kind should be standardized and expanded.

4. Integration of private sector performance data into federal situation understandings

A German Digital Supply Hub must be able to receive dynamic feedback from private sector systems – such as regarding the limited operational capability of a storage facility or the temporary unavailability of a service provider. This does not create operational control, but rather a reliable supply situation picture that can secure political decisions and specifically trigger coordinated measures.

5. Piloting along defined hub axes

With the aforementioned introduction of the maintenance and operation contract for several CSCs, the Bundeswehr has implemented an initial reliable solution for an advanced PMC. Now it is important to specifically further develop and scale PMC approaches. Along defined logistical-strategic axes, additional test fields should be created where data integration, contract mechanisms, and cooperation logics can be tested in different sectors (logistics, energy, IT, supply).

6. Development of a national cooperation model

In the long term, the German Digital Supply Hub should not act as a stand-alone solution, but should be embedded in a viable cooperation model between the state and private sector, which is also based on a regular culture of practice. The cooperation must bindingly regulate responsibilities, participation obligations, reporting procedures, activation logics, and utilization mechanisms – ideally through administratively agreed standard procedures and cross-sectoral governance bodies. In the long term, a nationwide architecture could emerge along the lines of the Comprehensive Defense Framework.

Creating these prerequisites is not a trivial matter. We are convinced that a series of similar studies is needed to accelerate the strategic integration of knowledge across all fields of Comprehensive Defense. In Germany, there are already initial examples, and as best practices from other NATO member states show, there are also solutions there that could be examined, adapted, and adopted. In addition, there is a variety of skills in the private sector that the Bundeswehr can rely on when implementing OPLAN DEU. The most important prerequisite for this is clear information about what is needed and when it is needed.

Appendix 1

Detailed Derivation of Prerequisites and Requirements

The following section provides a detailed description of the general requirements for successful PMC as outlined in Chapter 3. These requirements are derived from NATO frameworks, Bundeswehr specifications, and experiences from past crises.

1.1 Primacy of operational requirements: effectiveness before efficiency

In successful PMC, the fulfillment of operational requirements must be the very top priority. In the event of deployment, it is crucial that logistics effectively contribute to the success of the operation. Of course, this should be done as resource-efficiently as possible. Nevertheless, the primary goal of the PMC in this field must be effectiveness, not efficiency.

The NATO doctrine for logistics AJP-4 emphasizes:

> **"All logistic support efforts, from both the military and the civilian sector should be focused to satisfy the operational requirements necessary to guarantee the success of the [operation]."[26]**

Effectiveness clearly takes precedence over efficiency here as well, i.e., operational effectiveness is the central criterion of every PMC. The primacy of operational requirements thus forms the basis of the requirements framework.

1.2 Increase in operational capability

PMC must maximize the capabilities and potential of the deployed forces and material. Germany plays a central role as a logistical hub within NATO. Private sector capacities are indispensable in order to be able to deploy large troop contingents quickly in a crisis. Even today, the Bundeswehr relies almost exclusively on private sector service providers outside of crisis areas. The comparison of sizes alone makes it clear what influence civilian resources in logistics could have on the operational capability of the Bundeswehr: German road freight transport has around 3.83 million registered trucks,[27] while the entire logistics of the Bundeswehr only includes about 9,000 of its own vehicles and 18,000 employees.[28] By involving private sector providers, transport, maintenance, and support services could be outsourced, allowing military forces to remain available for core tasks. Should tension arise, this integration would also be absolutely necessary, as the Bundeswehr would then need all its own logistics forces to supply its own units, which in this scenario would not be stationed in Germany.

1.3 Clear control and responsibilities

Clear control structures, responsibilities, and decision-making paths are essential for a functioning PMC. Only when responsibilities are clearly defined can conflicts of objectives be avoided and responsiveness in crises ensured.

[26] NATO: Allied Joint Doctrine for Logistics (AJP-4), Edition B Version 1, Brussels 2012, p. 50, online: https://www.nato.int/docu/logi-en/logistics_hndbk_2012-en.pdf (accessed October 28, 2025).

[27] Federal Statistical Office of Germany (Destatis): Bestand an zulassungspflichtigen Lastkraftwagen in Deutschland, online: https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Transport-Verkehr/Unternehmen-Infrastruktur-Fahrzeugbestand/Tabellen/fahrzeugbestand.html (accessed October 28, 2025).

[28] DVZ – Deutsche Verkehrs-Zeitung: Wie die Zeitenwende die Logistik der Bundeswehr verändert, 2025, online: https://www.dvz.de/politik/detail/news/dvz-vor-ort-wie-die-zeitenwende-die-logistik-der-bundeswehr-veraendert.html (accessed October 28, 2025).

The NATO doctrine AJP-4 explicitly calls for clear responsibilities to be established for logistics:

"In order to develop a coherent logistic concept of operations, it is essential that guidelines be established to outline the responsibilities of each element as they relate to planning and conducting multinational logistic operations."[29]

This highlights the necessity for clear responsibility guidelines – between NATO commands, national authorities, and private sector actors. Only binding guidelines prevent overlaps, duplication, or gaps and ensure a coordinated approach. Clear governance structures create trust, reliability, and operational capability – they are thus a central prerequisite for effective PMC.

1.4 Interoperability and standardization

Uniform standards are a prerequisite for effective PMC. If all parties involved, be it the Bundeswehr, NATO partners, or private sector service providers, work according to uniform or coordinated procedures, cooperation becomes more efficient.

The NATO doctrine AJP-4.4 emphasizes:

"Standardization: Systems, data, software, procedures, and equipment must be standardised to facilitate interoperability and movement support."[30]

Standardization is not an end in and of itself, but a prerequisite for interoperability. In Germany, implementation is carried out through the STANAG agreements (standardization agreements of NATO), which establish binding technical and organizational minimum standards. This includes regulations for secure data exchange and for the compatibility of communication and logistics systems.

A central role is played by interoperability: Private sector and military systems must be technically and procedurally compatible with each other to seamlessly exchange information, resources, and processes. Standardized interfaces and coordinated data formats enable a common situational picture and coordinated control, e.g., of troop movements or supply along multinational corridors. Standardization and interoperability thus form the "common language" of successful PMC. They increase reliability, reduce friction losses, and ensure that military and private sector components seamlessly interact in complex operational scenarios.

[29] NATO: AJP-4 Allied Joint Doctrine for Logistics 2018, Chapter 2, 2.1, online: https://www.forsvaret.no/en/organisation/nduc/nodefic/pre-study-packages/NATO%201.06%20-%20Vedlegg%20AJP-4%20Doctrine%20for%20Logistics%20(2018).pdf (accessed October 28, 2025).

[30] NATO: AJP-4.4 Allied Joint Doctrine for Movement, Edition C, Version 1, September 2022, Chapter 1, Section 2, h, online: https://www.coemed.org/files/stanags/01_AJP/AJP-4.4_EDC_V1_E_2506.pdf (accessed October 28, 2025).

1.5 Security and compliance

Security and compliance form the foundation of every PMC. The integration of the Bundeswehr and private sector requires consistent adherence to military security standards by private sector partners. This concerns both the protection of classified information and technical and organizational measures to counteract cyber threats.

Current analyses of NATO procurements summarize the requirements as follows:

> **"Companies will likely have to adhere to NATO Security Policy, which in some cases mandates obtaining Facility Security Clearances (FSC) through national security authorities. Personnel involved … may need security clearances aligned with NATO Confidential or higher classification levels. Similarly, if triggered by a particular procurement opportunity, cybersecurity requirements under the NATO Cyber Defence Pledge would necessitate adherence to specific security protocols …".**[31]

Security and compliance are not just technical or administrative duties, but constitutive prerequisites for the integrity and functionality of the PMC.

1.6 Transparency and information situation: basis for control, situation assessment, and supply chain control

Transparency is a key requirement for effective PMC, serving as a foundation for a shared situational awareness and reliable decisions, both in the political arena and at the operational level. In complex deployment and crisis scenarios, military and private sector actors must have consistent, up-to-date, and reliable information. Only on this basis can priorities be set, resources be deployed in a targeted manner, and risks be identified early. Transparency is not an end in and of itself, but an expression of institutional trust-building and a prerequisite for operational effectiveness.

The NATO Allied Joint Doctrine for Civil-Military Cooperation (AJP-3.19) explicitly emphasizes this connection:

> **"Transparency helps instil trust, increases confidence and encourages mutual understanding. There is a need to demonstrate openness, integrity, competence, capability and resolve to gain respect, trust and confidence between all actors involved and thus create successful civil-military relationships."**[32]

[31] White & Case LLP: Navigating NATO Procurement: Legal and Regulatory Considerations for Companies in Finland & Sweden, March 23, 2025, online: https://www.whitecase.com/insight-alert/navigating-nato-procurement-legal-and-regulatory-considerations-companies-finland (accessed October 28, 2025).

[32] NATO: AJP-3.19 Allied Joint Doctrine for Civil-Military Cooperation, Edition A, Version 1, November 2018, Chapter 1, Section 5, pp. 1-6f, online: https://www.coemed.org/files/stanags/01_AJP/AJP-3.19_EDA_V1_E_2509.pdf (accessed October 28, 2025).

A resilient common situational understanding particularly requires structured information exchange on capacities, availabilities, bottlenecks, and risks, as far as this is compatible with security clearance regulations. The visibility of supply chains is equally essential. Only when inventories, means of transport, and goods flows can be tracked in real time is proactive control possible.

The NATO doctrine for logistics AJP-4 thus emphasizes:

> **"Visibility of logistic resources and capabilities is essential for effective and efficient logistic support … The key to this information is visibility on logistic requirements, resources, capabilities and processes."[33]**

In practice, this is done through systems like LOGFAS (Logistic Functional Area Services), which provide a common view of logistical resources within NATO. A comparable level of transparency should also be sought in the interaction between the Bundeswehr and private sector logistics companies. Only through transparent information exchange and complete visibility of logistical resources is a reliable information base created, which in turn is the prerequisite for coordinated decisions, operational control, and trustworthy PMC.

1.7 Robustness through dual structures and proactive planning

PMC must also function reliably under extreme conditions, even in case of failures, disturbances, or attacks. To ensure this, two elements are crucial: technical and structural redundancies and proactive, systematically anchored resilience planning. Both components pursue the same goal: Operational capability must be ensured even under difficult conditions.

NATO describes this requirement in its Allied Joint Doctrine AJP-01:

> **"Military resilience includes the forces being ready for employment with the capabilities and redundancy the military instrument requires to ensure its ability to absorb shocks, provide early resistance and conduct counter-offensive operations."[34]**

Redundancy and resilience are two sides of the same coin in this context. While redundancy creates operational security, resilience planning ensures strategic resilience. Only when both elements are integrated into the PMC can appropriate solutions remain operational and effective even in exceptional situations.

[33] NATO: AJP-4 Allied Joint Doctrine for Logistics, Edition B, Version 1, 2018, Chapter 1, Section 2, 1.11, online: https://www.forsvaret.no/en/organisation/nduc/nodefic/pre-study-packages/NATO%201.06%20-%20Vedlegg%20AJP-4%20Doctrine%20for%20Logistics%20(2018).pdf (accessed October 28, 2025).

[34] NATO: AJP-01 Allied Joint Doctrine, Edition F, Version 1, 2023, p. 21, online: https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf (accessed October 28, 2025).

Redundancies: reliability through dual structures

Redundancy describes the deliberate provision of alternative resources, paths, or systems to compensate for the failure of individual components without loss of functionality.

Specifically, this means: For critical logistical processes such as transportation, communication, or warehousing, alternative routes, alternative service providers, or reserve capacities must be planned and available. This is particularly true in an environment where, for example, bridges may fail, digital systems may be attacked, or transportation companies may be on strike.

Resilience: proactive risk management and crisis preparedness

While redundancy is central to mitigating acute failures, resilience planning aims at systematically preparing for complex disruptions. It includes, among other things, systematic and continuous preparation for potential failures, bottlenecks, or disruptions along the entire supply chain.

The NATO logistics guidelines (AJP-4) explicitly demand:

> **"The logistic risk must be continually assessed through the planning process so that appropriate mitigation can be designed into the plan to reduce the impact of logistic risk on operations."[35]**

At the same time, NATO emphasizes:

> **"Logistic support must be adaptive and flexible to be effective. Adequate planning allows NATO and nations to react in a timely manner to changes in the operational situation and/or requirements."**

Resilience therefore means not only precaution, but also the ability to quickly redirect through preparation, for instance when a supply route fails, new threat situations arise, or delivery bottlenecks occur.

[35] NATO: AJP-4 Allied Joint Doctrine for Logistics, Edition B, Version 1, 2018, Chapter 3, Section 3, pp. 3-4, online: https://www.forsvaret.no/en/organisation/nduc/nodefic/pre-study-packages/NATO%201.06%20-%20Vedlegg%20AJP-4%20Doctrine%20for%20Logistics%20(2018).pdf (accessed October 28, 2025).

Appendix 2

In-Depth Analysis of the Four Countries Selected as International Best Practices

Following the filtering of logistic hub states and institutionally secured PMCs, the four countries identified that already have mature, operationally robust cooperation mechanisms between state defense planning and private sector service providers will be examined in more detail below. The focus is on the practical integration of non-military infrastructures and supply sectors into national defense, especially in the energy, logistics, telecommunications, critical services, and IT sectors.

2.1 Netherlands

The Netherlands represents a central, logistical-geographical hub in the NATO context: Essential transport and transshipment processes for European supply routes run through the ports of Rotterdam and Vlissingen as well as Schiphol Airport. This distinguishes the Netherlands from Nordic countries like Finland, Sweden, or Norway: They do not primarily need to organize an immediate national defense, but rather secure the access of transatlantic forces towards Germany and Eastern Europe.

The Dutch model is based on a whole-of-society approach that systematically anchors the strong role of private sector operators in security preparedness. Around 80% of critical infrastructure is in private hands, which is why government and military entities can only access the necessary capacities through close cooperation.[36] This is coordinated by the Nationaal Coördinator Terrorismebestrijding en Veiligheid (National Coordinator for Counterterrorism and Security – NCTV), which ensures a situational picture shared between ministries, the military, and companies through the National Crisis Center (NCC) and the Nationaal Operationeel Coördinatiecentrum (National Operational Coordination Center – NOCC).

The involvement of the private sector takes place through sectoral laws, industry-specific self-commitments (covenants), and increasingly binding EU regulations (NIS2, CER). Thus, energy companies, logistics service providers, banks, and telecommunications providers are required to adhere to minimum standards and regularly conduct risk analyses and crisis exercises with government agencies.[37] Strategic stockpiling is partly organized through state-controlled but privately implemented structures, such as with oil and fuel reserves through the national agency COVA.[38]

Public–private platforms are particularly significant in the areas of port logistics, energy supply, and financial infrastructure. Emergency plans are developed, scenarios are played out, and communication channels are tested here in close coordination between the government and the private sector. Recently, an alliance of 22 public and private organizations was also founded, including companies such as KPN, Rabobank, Gasunie, TenneT, and the Port of Rotterdam, to further strengthen national resilience.[39]

The Netherlands makes clear that a country characterized by logistics can only fulfill its role as a hub if access to private sector capacities is subject to binding regulations. The state and military do not possess their own infrastructure reserves,

[36] NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid): Rollen en verantwoordelijkheden in de vitale infrastructuur, online: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/rollen-en-verantwoordelijkheden (accessed October 28, 2025).

[37] NCTV: AANPAK VITAAL – Vitale infrastructuur, online: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/aanpak-vitaal (accessed October 28, 2025).

[38] Algemene Rekenkamer: Strategische voorraden niet altijd aanwezig, September 29, 2022, online: https://www.rekenkamer.nl/actueel/nieuws/2022/09/29/rekenkamer-strategische-voorraden-niet-altijd-aanwezig (accessed October 28, 2025).

[39] Deloitte Netherlands: Publiek-private samenwerking voor een veilig en weerbaar Nederland, 2025, online: https://www.deloitte.com/nl/nl/about/press-room/publiek-private-samenwerking-voor-een-veilig-en-weerbaar-nederland.html (accessed October 28, 2025).

but instead rely on a network of companies that is prepared through regulation, cooperation platforms, and practice exercises. There is a direct connection to Germany in this regard: As a central NATO hub, it must – similarly to the Netherlands – ensure that private sector infrastructure and capacities are reliably available in the event of a defense scenario.

2.2 Finland

Finland has a highly developed national security system that consistently integrates private and military components. The conceptual basis is the principle of total defense (kokonaismaanpuolustus), which is based on the understanding that the resilience of society in the event of a defense scenario relies on cross-sectoral cooperation. The goal is to maintain critical infrastructures and supply systems in the event of tension or defense scenarios, also taking into account private sector stakeholders.[40]

The operational control of private sector–military cooperation processes is the responsibility of the National Emergency Supply Agency (NESA), a subordinate agency of the Finnish Ministry of Economic Affairs and Employment. NESA is responsible for developing sectoral contingency plans, coordinating with companies, and managing strategic reserves.[41]

The central legal basis is the Security of Supply Act (Laki huoltovarmuuden turvaamisesta), which obligates companies in selected sectors to participate in national security preparedness.[42] [43] Building on this, there are over 1,000 bilateral readiness agreements between NESA and private sector actors.[44]

These agreements include, among other things:

→ Transport logistics: e.g., provision of rail and truck capacities, access to driver pools and transshipment areas, emergency route planning with transport logistics companies.

→ Energy supply: including contractually secured fuel storage, refueling capacities, access to network infrastructure, cooperation with energy suppliers in contingency planning.

→ IT and telecommunications: such as the use of data centers, redundancy concepts for communication, physical and virtual network protection.

→ Food and pharmaceutical logistics: securing central supply chains, emergency reserves, as well as access to existing inventory systems of large retail chains or pharmaceutical wholesalers.

[40] BMVg: Deutschland und Finnland – Gemeinsamer Schutz der Ostsee, 2025, online: https://www.bmvg.de/de/aktuelles/deutschland-finnland-gemeinsamer-schutz-der-ostsee-5753460 (accessed October 28, 2025); Finnish Government: Government Defence Report outlines development of Finland's defence as part of NATO, online: https://valtioneuvosto.fi/en/-/government-defence-report-outlines-development-of-finland-s-defence-as-part-of-nato (accessed October 28, 2025).

[41] National Emergency Supply Agency (NESA): Homepage, online: http://www.nesa.fi/ (accessed October 28, 2025).

[42] NESA: Security of Supply Act on the Measures Necessary to Secure Security of Supply (Laki huoltovarmuuden turvaamisesta), English translation, online: https://www.huoltovarmuuskeskus.fi/en/organisation/funding-and-legislation/legislation (accessed October 28, 2025).

[43] Finnish Ministry of Economic Affairs and Employment: Government Report on Security of Supply, 2021, online: https://tem.fi/en/security-of-supply (accessed October 28, 2025).

[44] Finnish Ministry of Economic Affairs and Employment: Government Report on Security of Supply, 2021, online: https://tem.fi/en/security-of-supply (accessed October 28, 2025).

In each sector, Preparedness Committees are convened: industry-specific working groups consisting of representatives from government agencies, the military, regulatory authorities, and companies, who continuously conduct risk analyses, coordinate needs, and prepare concrete deployment scenarios.[45]

The Finnish system also relies on a national strategy for the storage of critical goods, which is controlled by NESA but largely implemented by private operators. State-defined minimum quantities apply for, among other things, fuels, grain, medicines, technical spare parts, and means of communication. The financing takes place within the framework of public–private mixed models; however, the inventories remain physically under the control of private sector actors.

A central element of resilience architecture is regular exercise practice. Companies with standby agreements are obliged to participate in scenario exercises and cross-sectoral simulations. In addition to technical parameters such as response times, failure logs, and availabilities, leadership and communication channels between private sector and military entities are also tested. NESA has established its own situation center for this purpose, which is networked with other authorities and the Ministry of Defense.[46]

Finland consistently demonstrates how private sector actors in critical sectors can be integrated into national security provision through regulatory assured, organizationally operationalized, and practically tested mechanisms. The ability to activate storage capacities, supply chains, energy flows, and IT infrastructure in the event of defense scenarios is not based on informal agreements, but on pre-established, verifiable agreements with clear escalation and leadership structures. For Germany, this results in a practical framework for the implementation of OPLAN DEU – particularly with regard to effective interface formation between military situation management and private sector provision in non-military sectors.

2.3 Sweden

The Swedish model of Total Defense (Totalförsvar) is based on a clear equality between private sector and military contributions to national resilience.[47] The strategy was reactivated in 2015 after nearly two decades of reduced defense planning due to the security policy developments in the Baltic Sea region and has been gradually embedded in legislation and administrative structures since 2017. The cross-departmental planning framework obligates central authorities to participate in defense preparedness and includes private operators of critical infrastructures through sector-specific regulations and agreements. The basis is the national security resolution of the parliament (Totalförsvarsbeslutet), which is regularly updated.

The operational control is carried out by the Swedish Civil Contingencies Agency (MSB, Myndigheten för samhällsskydd och beredskap), which is coordinated with the Ministry of Defense, regional administrative authorities, and military command headquarters. The MSB publishes binding guidelines and sector strategies for contingency planning, including, among others,

[45] Prime Minister's Office Finland: Preparedness and comprehensive security in Finland, online: https://valtioneuvosto.fi/documents/10616/622966/J1811_Preparedness+and+comprehensive+security.pdf (accessed October 28, 2025).

[46] Kähkönen, Aku-M.; Forsberg, Robin: Preparing for a rainy day: What can EU member states learn from Finland's approach to resilience?, oiip Policy Analysis 5/2024, online: https://www.oiip.ac.at/en/publications/preparing-for-a-rainy-day-what-can-eu-member-states-learn-from-finlands-approach-to-resilience/ (accessed October 28, 2025).

[47] Government Offices of Sweden: Total Defense – Government Policy, online: https://www.government.se/government-policy/total-defense/ (accessed October 28, 2025).

the framework regulations for operators of critical infrastructures, which are available on the authority's website.[48]

Private sector involvement is not optional, but rather mandated by law. Companies in selected sectors, particularly energy, telecommunications, transport, IT, food supply, and financial services, are required to take preparatory measures. These include:

→ development and implementation of operational contingency plans that must be coordinated with regional authorities,

→ proof of redundancies (e.g., emergency power supply, data mirroring, alternative means of transport),

→ physical availability and access to critical resources (e.g., water, fuel, storage areas),

→ participation in situation briefings, staff framework exercises, and interdepartmental coordination formats,

→ integration in Samverkansområden, which are permanent cooperation platforms for authorities, companies, and armed forces.

A key component of the model is the regular involvement of private sector actors in comprehensive defense exercises.[49] The most extensive implementation to date was the "Totalförsvarsövning 2020" (TFÖ 20), which for the first time since the Cold War simulated a comprehensive defense scenario at national level. Over 400 organizations participated in the exercise, including numerous private operators from the fields of energy, food retail, telecommunications, and IT.[50]

The MSB has established its own coordination structure for business in the context of Total Defense. Known as the Företagsnätverk för beredskap (preparedness network for businesses), it serves as an interface for industry-specific communication, knowledge transfer, and early warning. This network includes several hundred organizations that are regularly involved in scenario planning, training, and strategic consulting.[51]

In addition, the national Försörjningsberedskap (provision preparedness) has been systematically sectorized and supported with legally secured target figures. Companies can receive incentives through government funding to maintain stockpiling or redundancy measures – this includes, for example, IT capacities, drug supplies, or regional fuel depots. In selected cases, bilateral performance agreements exist between ministries and large companies.[52]

The integration of business takes place both vertically (between national strategy, regional administration, and operational implementation) and horizontally (within industry clusters through associations and cooperation platforms). The escalation logic is multi-level: In basic operations, companies are responsible for this themselves, with oversight by the MSB; in the event of a crisis, emergency regulations come into play, in which the state can gain access to resources and networks.

[48] Myndigheten för samhällsskydd och beredskap (MSB): Homepage, online: https://www.msb.se/en/ (accessed October 28, 2025).

[49] Krisinformation.se: Totalförsvarsövning, online: https://www.krisinformation.se/forbered-dig/handelser-och-storningar/2019/tfo-2020 (accessed October 28, 2025)

[50] Swärd, Ann-Margreth: Private-Public Collaboration in Sweden's Civil Preparedness, Swedish Defence University, 2023, online: https://fhs.diva-portal.org/smash/get/diva2:1831504/FULLTEXT01.pdf (accessed October 28, 2025).

[51] MSB: Företagsnätverket för beredskap, online: https://www.msb.se/sv/utbildning--ovning/natverk-och-samverkan/foretagsnatverket-for-beredskap/ (accessed October 28, 2025).

[52] MSB: Företagens roll i totalförsvaret – Inspiration, vägledning och riktlinjer, MSB 0052-21, 2021, online: https://rib.msb.se/filer/pdf/30803.pdf (accessed October 28, 2025).

Sweden represents a decentralized but strongly state-structured model of private sector involvement in military defense planning. The role of companies is clearly operationalized through legal obligations, strategic consulting, and exercise integration. For OPLAN DEU, the combined consideration of federally designed responsibility diffusion and central control by a specialized agency (MSB) is particularly applicable – as is the idea of sectoral corporate networks as early warning and action units in national crisis prevention.

2.4 United Kingdom

Unlike Finland and Sweden, the United Kingdom does not pursue a formalized total defense approach, but it does have a highly developed system of contractually regulated collaborations between the Ministry of Defence (MoD) and private sector service providers. The basis is the strategic concept of the "Whole Force," which considers military personnel, civil state resources, and private contractors as equivalent elements of a comprehensive national defense system. [53] This logic is applied in the United Kingdom not only to classic armament tasks, but explicitly also to logistics-related support areas, infrastructure, IT, and transport.

A central role is played by the contractual involvement of private sector partners in the operational support of military missions. For example, the strategic air transport and air refueling capacity of the British armed forces is provided by the private consortium AirTanker. It operates a fleet of Airbus A330 MRTT aircraft, which are used for civilian purposes under normal operations and can be fully militarily activated in a crisis. The crews partly consist of civilian employees, who are simultaneously listed as what are known as Sponsored Reserves and can be activated in case of deployment.[54] Sponsored Reserves are civilian employees who are militarily trained and registered and can be activated if necessary.

In the field of maritime logistics, the United Kingdom has the STUFT system (Ships Taken Up From Trade), which includes a prioritized list of private commercial ships that can be contractually bound and made available in the event of a defense situation. This concept was historically successfully used in the Falklands War and is still an integral part of military mobility planning.[55]

In addition, the UK Ministry of Defence maintains extensive framework agreements with companies for logistical services, site operation, maintenance, and material management. These include, among others, the companies Babcock[56], Serco, DHL, and KBR. These companies operate, among other things, military depots, vehicle parks, storage areas, medical facilities, and data infrastructure on behalf of the MoD – both in basic operations and under operational conditions.

A specific instrument for the integration of private sector workforce expertise is the aforementioned concept of Sponsored Reserves. These are civilian employees of partner firms who are trained and registered militarily in their role. In case of need, they can be temporarily activated and integrated into military command structures for

[53] UK Ministry of Defence: Defence Industrial Strategy – Statement of Intent, 2025, online: https://www.gov.uk/government/publications/defence-industrial-strategy-statement-of-intent/defence-industrial-strategy-statement-of-intent (accessed October 28, 2025).

[54] AirTanker: What we do – Civil Flying, online: https://www.airtanker.co.uk/about/what-we-do/civil-flying/ (accessed October 28, 2025).

[55] UK Ministry of Defence: Defense Support Strategy, 2022, online: https://www.gov.uk/government/publications/defence-support-strategy (accessed October 28, 2025).

[56] Babcock International: FY25 Statement, June 25, 2025, p. 25, online: https://www.babcockinternational.com/wp-content/uploads/2025/06/Babcock-FY25-statement-25.06.25.pdf (accessed October 28, 2025).

defined purposes, such as system administration, maintenance, or communication.

Since 2023, this cooperative approach has been extended to private sector operators of critical infrastructure under the new UK Government Resilience Framework. For the first time, the strategy defines systematic communication and cooperation obligations between state security agencies and companies in the fields of energy, water, IT, health, and transport. The goal is to improve responsiveness to hybrid threats and combined crisis situations. The responsible ministries receive uniform guidelines for cross-sector coordination and crisis communication.[57]

The United Kingdom demonstrates how private sector performance can be integrated into the overall national defense logic through long-term contractual commitment, personnel integration (Sponsored Reserves), and function-related mobilization planning – without a formal total defense architecture. Particularly adaptable for Germany are models of operational responsibility sharing, for example in the area of infrastructure and warehouse operations, as well as the use of private transport means on a contractual basis. The British approach shows that high operational resilience can be achieved through professional partnership models between the state and the private sector – provided that clear responsibilities, escalation procedures, and role definitions are systematically implemented.

[57] UK Cabinet Office: UK Government Resilience Framework, 2023, online: https://www.gov.uk/government/publications/resilience-framework (accessed October 28, 2025).

List of References

AirTanker: What we do – Civil Flying, online: https://www.airtanker.co.uk/about/what-we-do/civil-flying/ (accessed October 28, 2025).

Algemene Rekenkamer: Strategische voorraden niet altijd aanwezig. September 29, 2022, online: https://www.rekenkamer.nl/actueel/nieuws/2022/09/29/rekenkamer-strategische-voorraden-niet-altijd-aanwezig (accessed October 28, 2025).

Babcock International: FY25 Statement. June 25, 2025, p. 25, online: https://www.babcock-international.com/wp-content/uploads/2025/06/Babcock-FY25-statement-25.06.25.pdf (accessed October 28, 2025).

Bundesregierung: Nationale Sicherheitsstrategie der Bundesrepublik Deutschland, online: https://www.nationalesicherheitsstrategie.de/ (accessed October 28, 2025).

Bundesverband Materialwirtschaft, Einkauf und Logistik e. V. (BME): BME-Logistikstudie 2024 – Risikomanagement und Resilienz in Supply Chains, Eschborn 2024, online: https://www.bme.de/fachinformationen/bme-logistikstudie-2024/ (accessed October 28, 2025).

Bundeswehr: Operationsplan Deutschland (OPLAN DEU): Deutschland gemeinsam verteidigen. Operatives Führungskommando der Bundeswehr, online: https://www.bundeswehr.de/de/organisation/operatives-fuehrungskommando-der-bundeswehr/auftrag-und-aufgaben/operationsplan-deutschland (accessed October 28, 2025).

BwConsulting: Landes- und Bündnisverteidigung – Framework „Comprehensive Defence für Deutschland“, online: https://www.bwconsulting.de/lvbv/ (accessed October 28, 2025).

Defense Logistics Agency (DLA): Logistics across Norway for Cold Response, online: https://www.dla.mil/About-DLA/News/News-Article-View/Article/2124356/logistics-across-norway-for-cold-response/ (accessed October 28, 2025).

Deloitte Nederland: Publiek-private samenwerking voor een veilig en weerbaar Nederland, 2025, online: https://www.deloitte.com/nl/nl/about/pressroom/publiek-private-samenwerking-voor-een-veilig-en-weerbaar-nederland.html (accessed October 28, 2025).

Deutscher Bundestag: Regierungsbefragung im Wortlaut, June 5, 2024, online: https://www.bundestag.de/dokumente/textarchiv/2024/kw23-de-regierungsbefragung-1002264 (accessed October 28, 2025).

DVZ – Deutsche Verkehrs-Zeitung: Wie die Zeitenwende die Logistik der Bundeswehr verändert, 2025, online: https://www.dvz.de/politik/detail/news/dvz-vor-ort-wie-die-zeitenwende-die-logistik-der-bundeswehr-veraendert.html (accessed October 28, 2025).

European Parliament: EU Military Mobility Action Plan & CEF 2023–2027, EPRS_BRI(2025)775860, online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775860/EPRS_BRI(2025)775860_EN.pdf (accessed October 28, 2025).

Finnish Government: Government Defence Report outlines development of Finland's defence as part of NATO, online: https://valtioneuvosto.fi/en/-/government-defence-report-outlines-development-of-finland-s-defence-as-part-of-nato (accessed October 28, 2025).

Finnish Ministry of Economic Affairs and Employment: Government Report on Security of Supply, 2021, online: https://tem.fi/en/security-of-supply (accessed October 28, 2025).

German Federal Office of Civil Protection and Disaster Assistance (BBK): Zivil-Militärische Zusammenarbeit, online: https://www.bbk.bund.de/DE/Themen/Krisenmanagement/Zivil-Militaerische-Zusammenarbeit/zivil-militaerische-zusammenarbeit_node.html (accessed October 28, 2025).

German Federal Ministry of the Interior (BMI): Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien (RRGV), online: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/RRGV.html (accessed October 28, 2025).

German Federal Ministry of Defence (BMVg): Deutschland und Finnland – Gemeinsamer Schutz der Ostsee, 2025, online: https://www.bmvg.de/de/aktuelles/deutschland-finnland-gemeinsamer-schutz-der-ostsee-5753460 (accessed October 28, 2025).

German Federal Ministry of Defence (BMVg): NATO Force Model – Wie Deutschland sich ab 2025 engagiert, online: https://www.bmvg.de/de/aktuelles/nato-force-model-wie-deutschland-sich-ab-2025-engagiert-5465714 (accessed October 28, 2025).

German Federal Ministry of Defence (BMVg): Neuer Wehrdienst für Deutschland, online: https://www.bmvg.de/de/neuer-wehrdienst (accessed October 28, 2025).

German Federal Ministry of Defence (BMVg): Verteidigungspolitische Richtlinien 2023, online: https://www.bmvg.de/de/aktuelles/verteidigung-spolitische-richtlinien-2023-veroeffentlicht-5701338 (accessed October 28, 2025).

German Federal Ministry of Defence (BMVg): Wehrwissenschaftliche Forschung – Jahresbericht 2024, online: https://www.bmvg.de/resource/blob/6001656/8b2973bb7908f6e09e0dd3bd-1ed1e827/wehrwissenschaftliche-forschung-data.pdf (accessed October 28, 2025).

German Federal Ministry of Defence (BMVg): Zeitenwende – Grundsatzdokumente und strategische Neuaufstellung, online: https://www.bmvg.de/de/themen/sicherheitspolitik/zeitenwende (accessed October 28, 2025).

Government Offices of Sweden: Total Defence – Government Policy, online: https://www.government.se/government-policy/total-defence/ (accessed October 28, 2025).

Kähkönen, Aku-M.; Forsberg, Robin: Preparing for a rainy day: What can EU member states learn from Finland's approach to resilience? oiip Policy Analysis 5/2024, online: https://www.oiip.ac.at/en/publications/preparing-for-a-rainy-day-what-can-eu-member-states-learn-from-finlands-approach-to-resilience/ (accessed October 28, 2025).

Krisinformation.se: Totalförsvarsövning 2020, online: https://www.krisinformation.se/forberedd-ig/handelser-och-storningar/2019/tfo-2020 (accessed October 28, 2025).

McKinsey & Company: Supply chains to build resilience, manage proactively, online: https://www.mckinsey.com/capabilities/operations/our-insights/supply-chains-to-build-resilience-manage-proactively (accessed October 28, 2025).

MHP Management- und IT-Beratung GmbH: Digitale Zwillinge – Neue Perspektiven für Lieferketten, white paper, March 2024, online: https://www.mhp.com/fileadmin/www.mhp.com/downloads/whitepaper/MHPWhitePaper_DigitalTwins_DE.pdf (accessed October 28, 2025).

Myndigheten för samhällsskydd och beredskap (MSB): Företagens roll i totalförsvaret – Inspiration, vägledning och riktlinjer. MSB 0052-21, 2021, online: https://rib.msb.se/filer/pdf/30803.pdf (accessed October 28, 2025).

Myndigheten för samhällsskydd och beredskap (MSB): Företagsnätverket för beredskap, online: https://www.msb.se/sv/utbildning--ovning/natverk-och-samverkan/foretagsnatverket-for-beredskap/ (accessed October 28, 2025).

Myndigheten för samhällsskydd och beredskap (MSB): Homepage, online: https://www.msb.se/en/ (accessed October 28, 2025).

National Emergency Supply Agency (NESA): Homepage, online: http://www.nesa.fi/ (accessed October 28, 2025).

National Emergency Supply Agency (NESA): Security of Supply Act (Laki huoltovarmuuden turvaamisesta), English translation, online: https://www.huoltovarmuuskeskus.fi/en/organisation/funding-and-legislation/legislation (accessed October 28, 2025).

NATO: AJP-01 Allied Joint Doctrine. Edition F, Version 1, 2023, online: https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf (accessed October 28, 2025).

NATO: AJP-4 Allied Joint Doctrine for Logistics 2018, online: https://www.forsvaret.no/en/organisation/nduc/nodefic/pre-study-packages/NATO%201.06%20-%20Vedlegg%20AJP-4%20Doctrine%20for%20Logistics%20(2018).pdf (accessed October 28, 2025).

NATO: AJP-4.4 Allied Joint Doctrine for Movement, Edition C, Version 1, September 2022, online: https://www.coemed.org/files/stanags/01_AJP/AJP-4.4_EDC_V1_E_2506.pdf (accessed October 28, 2025).

NATO: Topic: Strengthening NATO's eastern flank, online: https://www.nato.int/cps/en/natohq/topics_136388.htm (accessed October 28, 2025).

NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid): AANPAK VITAAL – Vitale infrastructuur, online: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/aanpak-vitaal (accessed October 28, 2025).

NCTV: Rollen en verantwoordelijkheden in de vitale infrastructuur, online: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/rollen-en-verantwoordelijkheden (accessed October 28, 2025).

Prime Minister's Office Finland: Preparedness and comprehensive security in Finland, online: https://valtioneuvosto.fi/documents/10616/622966/J1811_Preparedness+and+comprehensive+security.pdf (accessed October 28, 2025).

Rheinmetall AG: Rheinmetall gewinnt Auftrag zur logistischen Unterstützung der Streitkräfte, press release, February 19, 2025, online: https://www.rheinmetall.com/de/media/news-watch/news/2025/02/2025-02-19-rheinmetall-gewinnt-auftrag-zur-logistischen-unterstuetzung-der-streitkraefte (accessed October 28, 2025).

Roman, D.; Schneider, M.; et al.: Digital Twins for Supply Chain Simulation: Methods and Applications. In: Logistics 2025, 9(1), 22, online: https://doi.org/10.3390/logistics9010022 (accessed October 28, 2025).

Siemens AG; Frost & Sullivan: Building Sustainable and Agile Industrial Supply Chain, Munich, 2021, online: https://assets.new.siemens.com/siemens/assets/api/uuid:a63fafc9-5d55-48ba-89e7-5d58c4bfb87d/Building-sustainable-agile-industrial-supply-chain-Frost-Sullivan-_original.pdf (accessed October 28, 2025).

Statistisches Bundesamt (Destatis): Bestand an zulassungspflichtigen Lastkraftwagen in Deutschland, online: https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Transport-Verkehr/Unternehmen-Infrastruktur-Fahrzeugbestand/Tabellen/fahrzeugbestand.html (accessed October 28, 2025).

Stiftung Wissenschaft und Politik (SWP): Die Nato nach dem Gipfel von Madrid, SWP-Aktuell 2022/A 49, online: https://www.swp-berlin.org/10.18449/2022A49/ (accessed October 28, 2025).

Swärd, Ann-Margreth: Samverkan i en totalförsvarsövning – Regionens roll vid TFÖ 20. Führungsakademie der Verteidigung, 2023, online: https://fhs.diva-portal.org/smash/get/diva2:1831504/FULLTEXT01.pdf (accessed October 28, 2025).

UK Cabinet Office: UK Government Resilience Framework, 2023, online: https://www.gov.uk/government/publications/resilience-framework (accessed October 28, 2025).

UK Ministry of Defence: Defence Support Strategy, 2022, online: https://www.gov.uk/government/publications/defence-support-strategy (accessed October 28, 2025).

UK Ministry of Defence: Defence Industrial Strategy – Statement of Intent, 2025, online: https://www.gov.uk/government/publications/defence-industrial-strategy-statement-of-intent/defence-industrial-strategy-statement-of-intent (accessed October 28, 2025).

U.S. Army: Defender Europe 21 – Solidarity on the Move, online: https://www.army.mil/article/252655/defender_europe_21_solidarity_on_the_move (accessed October 28, 2025).

German Association of the Automotive Industry (VDA): Basic principles of collaboration between automobile manufacturers and their partners, 2022, online: https://www.vda.de/dam/

jcr:b531a4a2-8873-4c84-8bd2-78ebd3078862/VDA_5867_Grundsatzpapier_für_den_HG_III_Vorstand_RZ2.pdf (accessed October 28, 2025).

White & Case LLP: Navigating NATO Procurement: Legal and Regulatory Considerations for Companies in Finland & Sweden, March 23, 2025, online: https://www.whitecase.com/insight-alert/navigating-nato-procurement-legal-and-regulatory-considerations-companies-finland (accessed October 28, 2025).

Bundeswehr Centre of Military History and Social Sciences (ZMSBw): Schichttorte Vorneverteidigung Kalter Krieg, online: https://zms.bundeswehr.de/de/mediathek/aktuelle-karte-schichttorte-vorneverteidigung-kalter-krieg-5533640 (accessed October 28, 2025).

About MHP

MHP Management- und IT-Beratung GmbH

MHP is a German management and IT consultancy headquartered in Ludwigsburg.

For nearly three decades, the company has been driving the transformation of processes and products for around 300 clients worldwide. As a trusted partner in the automotive, manufacturing, aerospace, public, and defense sectors, MHP supports its clients in strategy and IT transformations across the entire value chain. A subsidiary of Porsche AG, the company provides both strategic and operational consulting in key areas such as factory planning, supply chain management, integration and scaling, cybersecurity, artificial intelligence, program management, and platforms & ecosystems. The goal is to sustainably enhance speed, sovereignty, and resilience. With around 4,700 employees worldwide, MHP is united by a shared commitment to excellence and long-term success. This ambition continues to drive the company – today and in the future.

mhp.com/newsroom

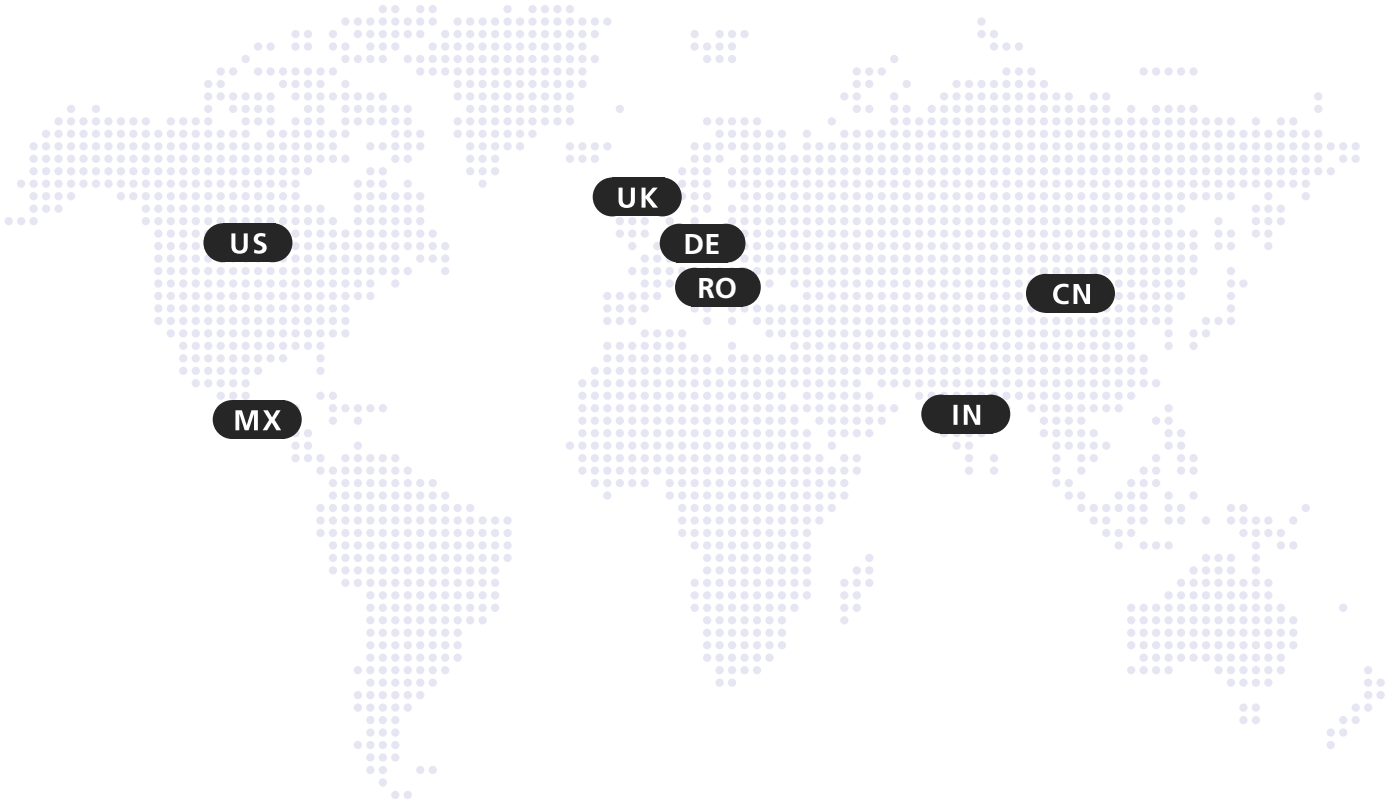
Sponsor
Henning M. Schulze
Partner
International & Global Sourcing
henning.schulze@mhp.com

Contact Person
John Claudius Eisenhauer
Partner
Sector Lead Public & Defense
john.eisenhauer@mhp.com

Layout and Design: www.freiland-design.de

Adobe Stock Photo Credits: Cover Arif Hama // p. 7 Artinun // p. 22 Hero Design // p. 33 Kirill Gorlov // p. 38 Ilja // p. 54 peopleimages.com // p. 68 Synthetic creator // p. 80 abu

ENABLING YOU TO SHAPE A BETTER TOMORROW



mhp.com