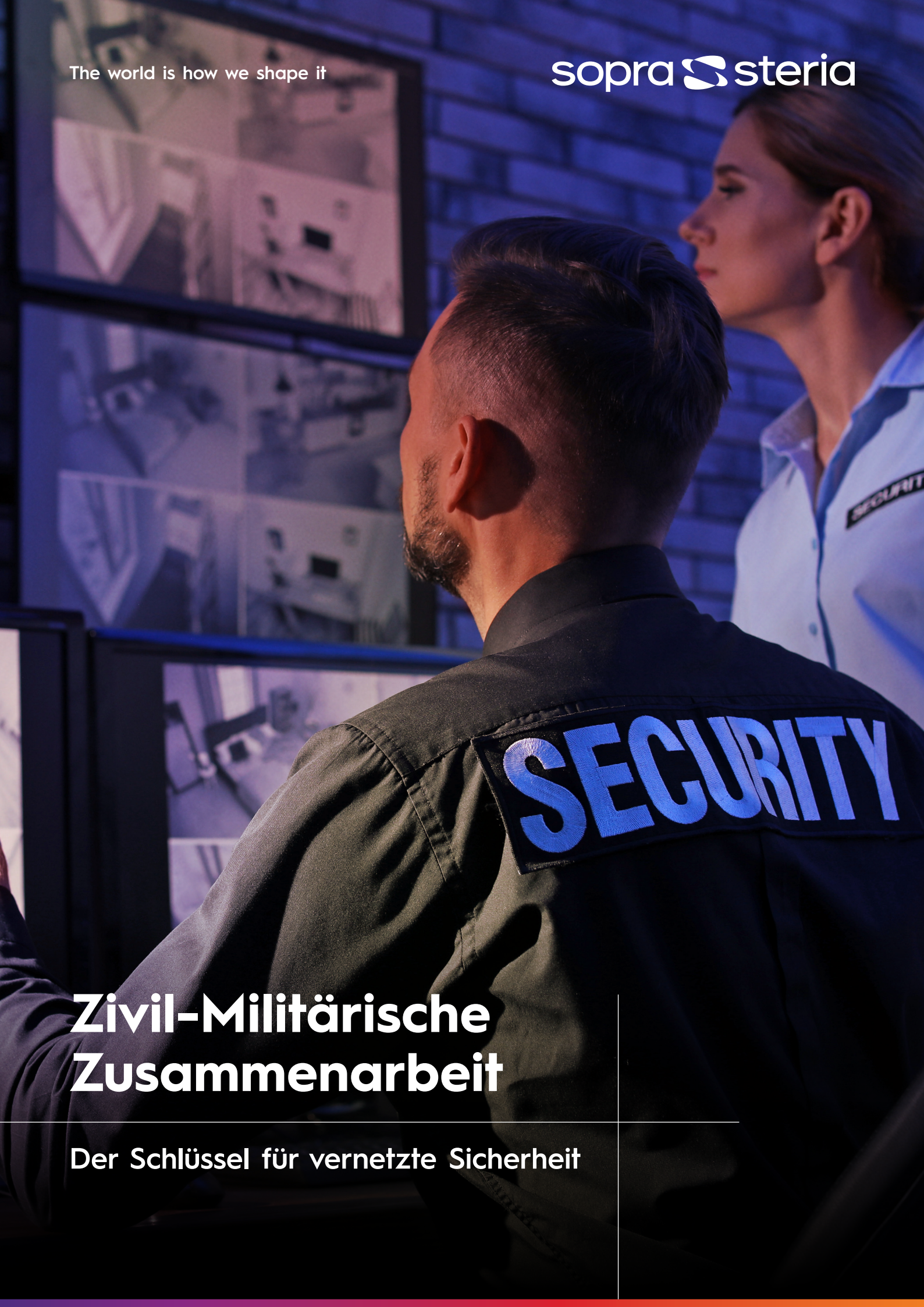
The world is how we shape it

sopra steria



Zivil-Militärische Zusammenarbeit

Der Schlüssel für vernetzte Sicherheit

Was ist Zivil-Militärische Zusammenarbeit?

Die Zivil-Militärische Zusammenarbeit (ZMZ) bezeichnet das abgestimmte Zusammenwirken ziviler und militärischer Akteure zur Unterstützung der gesamtstaatlichen Sicherheitsvorsorge in Friedenszeiten und im Verteidigungsfall. Laut den Verteidigungspolitischen Richtlinien 2023 ist sie ein zentrales Element der „Integrierten Sicherheit" im Sinne eines Comprehensive Defence-Verständnisses. ZMZ dient der gegenseitigen Verstärkung militärischer Fähigkeiten und ziviler Ressourcen, insbesondere. in den Bereichen Führung, Logistik, Infrastruktur, Versorgung, Kommunikation und Schutz kritischer Infrastruktur. Sie soll staatliche Handlungsfähigkeit auch dann erhalten, wenn die Bundeswehr im Landes- und Bündnisverteidigungsfall operativ gebunden ist.

Was ist neu an ZMZ 4.0?

Das Grünbuch ZMZ 4.0 (2024) beschreibt die ZMZ 4.0 als dauerhaft verankerte Fähigkeit zur Unterstützung der Landes- und Bündnisverteidigung in hybriden Bedrohungslagen. Im Mittelpunkt stehen die frühzeitige Integration ziviler Akteure, die Vernetzung von Führungsstrukturen sowie der systematische Schutz kritischer Infrastrukturen. ZMZ 4.0 wird damit zu einem tragenden Element einer gesamtstaatlichen Resilienz-Architektur.

Säulen der Gesamtverteidigung

Die Gesamtverteidigung ruht auf zwei strategischen Säulen:

- **Zivile Verteidigung** mit den vier Funktionsbereichen staatliche Handlungsfähigkeit, Bevölkerungsschutz, Versorgungssicherheit, militärische Unterstützungsleistungen.
- **Militärische Verteidigung,** verstanden als Landes- und Bündnisverteidigung – wie in den Verteidigungspolitischen Richtlinien 2023 und im OPLAN DEU verankert.

ZMZ verbindet die Verteidigungssäulen operativ und trägt signifikant zur Gesamtfunktionalität gesamtstaatlicher Sicherheitsstrukturen bei.

Handlungsfelder der ZMZ

Zur Förderung der technischen, organisatorischen und kommunikativen Leistungsfähigkeit der ZMZ in den Krisenphasen Vorbereitung, Vorsorge, Schutz, Reaktion und Regeneration identifizieren wir fünf zentrale Handlungsfelder:

1. Führungsfähigkeit und Kommunikation:

Gemeinsame Lagebilder, verzahnte Entscheidungsstrukturen und Digitalplattformen ermöglichen Koordination in Echtzeit.

2. IT- und Cybersicherheit:

Harmonisierte Schutzstandards, Cyberabwehrstrukturen und gemeinsame Krisenreaktionszentren stärken die Immunität gegen hybride Angriffe.

3. Datenmanagement und Lagebilder:

Auswertung und Verteilung sicherheitsrelevanter Informationen aus den Bereichen Zivilschutz, Polizei und Streitkräfte erfordern vernetzte Systeme.

4. Schutz Kritischer Infrastrukturen (KRITIS):

Zivile und militärische Akteure müssen die kritischen Infrastrukturen Deutschlands gemeinsam absichern und aufrechterhalten.

5. Logistik und Mobilität:

Wachsende Bedarfe an multimodaler Vorhaltung, Verlegung und Steuerung von Material und Ressourcen erfordern integrative Logistikansätze.

Annahmen für die wirksame Ausgestaltung der Handlungsfelder

Wir gestalten die identifizierten Handlungsfelder auf Basis folgender Annahmen aus:

ZMZ politisch langfristig priorisiert:

Die Bundesregierung sieht die gesamtstaatliche Sicherheitsvorsorge als Kernthema. Der politische Wille zur Stärkung der Bundeswehr und zur institutionellen ZMZ-Verankerung (z. B. Nationaler Sicherheitsrat) ist stabil.

Mittelfristig ausreichende finanzielle Mittel verfügbar:

Der Koalitionsvertrag sieht massive staatliche und private Investitionen in die Verteidigungsindustrie vor. Die Finanzierung sicherheitspolitischer Maßnahmen auch im zivilen Bereich ist gesichert.

Technologische Interoperabilität realistisch umsetzbar:

Die Digitalisierung von Streitkräften und Krisenkommunikation hat hohe Priorität. Es ist realistisch, dass bestehende Führungs- und IT-Systeme interoperabel weiterentwickelt werden.

Rechtlicher Rahmen reformbereit:

Aktuelle Rechtsgrundlagen der ZMZ werden bzgl. Zuständigkeiten, Datenaustausch und, föderaler Koordination wirksam weiterentwickelt.

Beteiligung wächst:

Die breite sicherheitspolitische Debatte lässt die Beteiligungsbereitschaft zivilgesellschaftlicher, wirtschaftlicher und föderaler Akteure ansteigen.

Ansätze und Anwendungsbeispiele zur Ausgestaltung der Handlungsfelder

Welche Ansätze und Maßnahmen helfen nun auf dieser Annahmenbasis bei der konkreten Ausgestaltung der Handlungsfelder weiter?

Handlungsfeld 1: Führungsfähigkeit und Kommunikation

Geht das Vertrauen in die Funktionalität von Führungsstrukturen verloren, werden staatliche, ökonomische und gesellschaftliche Strukturen destabilisiert. Die Angriffsvektoren auf Führungsstrukturen sind in der heutigen hybriden Bedrohungslage mehrdimensional und reichen von Cyberangriffen über gezielte, langfristig angelegte Desinformationskampagnen bis hin zur Androhung oder Ausübung lebensbedrohlicher Gewalt (z. B. Rheinmetall-Anschlagsplan-Papperger oder Taurus-Abhöraffäre).

Verlässliche Führungsfähigkeit ist die Grundvoraussetzung, um Schutz-, Hilfs- und Gegenmaßnahmen im Falle einer Eskalation, einer Krise oder eines Krieg koordinieren und steuern zu können. Unser **gesamtgesellschaftlicher Anspruch** muss es sein, dass diese Fähigkeit heute weder an den Zuständigkeitsgrenzen von Behörden, Ministerien oder Unternehmen noch geographisch an den Grenzen der Bundesländer oder des Landes endet. Essenzielle Instrumente der Führungsfähigkeit sind ein integriertes und **interdisziplinäres Lagebild, hochverfügbare, sichere Kommunikationsmittel und IT sowie für erwartbare Szenarien vorbereitete Kommunikationsstrategien.** Dazu kommen eindeutig geregelte und den Betroffenen bekannte territoriale Zuständigkeiten sowie klare prozessuale und organisatorische Verantwortlichkeiten.

Das regelmäßige Üben der Führungsprozesse entlang der erwartbaren Szenarien ist unerlässlich. Denn auch Üben kann abschrecken, wenn erfolgreich aufgezeigt wird, dass Deutschland und die EU über gehärtete Führungsstrukturen und -instrumente verfügen, mit denen Krisensituationen dauerhaft durchhaltefähig bewältigt werden können. Ein „Warntag" ist immerhin ein Anfang, um der Gesellschaft und dem Einzelnen eine initiale Orientierung für den Ernstfall zu geben. Aber: Was folgt eigentlich auf die Warnung?

Die Digitalisierung bietet u. a. viele Möglichkeiten der **Simulation von Szenarien** und der Bereitstellung von **virtuellen Trainings.** Darin liegt die große Chance, schnell und mit großer Reichweite die Führungsfähigkeit verantwortlicher Stellen (Ministerien, Behörden, Institutionen und Unternehmen) innerhalb der eigenen Organisation und untereinander mit Fokus auf diversen Bedrohungsszenarien erproben, konsequent weiterentwickeln und härten zu können. Die Digitalisierung bietet das Potenzial zur Bürgereinbeziehung.

„Führung beginnt mit Klarheit. Und Klarheit beginnt mit einem gemeinsamen Lagebild."

RON DE JONGE
Head of Public Sector
Sopra Steria

Handlungsfeld 2:
IT- und Cybersicherheit

Der russische Angriffskrieg auf die Ukraine zeigt, dass physische Wirkmittel in der hybriden Kriegsführung von Aktivitäten im Cyberraum flankiert werden. Cyberangriffe gehören längst zum Repertoire staatlicher Akteure. Gemeinsam mit offensiven Aktivitäten von organisierten Kriminellen steigt die Bedrohungslage in Deutschland seit Jahren. Ziele sind finanzielle Bereicherung, Informationsdiebstahl (Patente, Operationspläne), Sabotage an der Infrastruktur sowie gezielte Desinformation der Bevölkerung.

Um Cyberangriffe schnellstmöglich zu erkennen und angemessen reagieren zu können, sind ein **behördenübergreifendes Lagebild** und **abgestimmte Reaktionen** unerlässlich. Dazu müssen Meldewege etabliert sein und genutzt werden. Das nationale Cyber-Abwehrzentrum (Cyber-AZ) als koordinierende Stelle für die Zusammenarbeit von Behörden, das CERT-Bund und die Aufwertung des CIR (Cyber- und Informationsraum) als vollwertiger Teilstreitkraft waren hierfür wichtige Schritte. Das Ausrufen der Cybernation Deutschland unterstreicht die strategische Bedeutung im Rahmen der ZMZ.

Die ISO 27001, der IT-Grundschutz des BSI und die NIS-2-Richtlinie definieren wichtige Anforderungen an Organisationen und deren Cybersicherheit. Hierbei spielen **Security Operation Center der nächsten Generation (NextGen SOC)** eine Schlüsselrolle, besonders wenn diese über Schnittstellen an staatliche Meldesysteme angebunden werden können, um schnellstmöglich Angriffe in der Fläche zu identifizieren. Außerdem gilt es, innovative Ansätze für die Cyberabwehr zu entwickeln. So kann die Sicherheit von Informationen durch Ansätze wie **Data-Centric Security (DCS)** neu gedacht werden. Gemeinsame Planspiele und Notfallübungen müssen im Falle eines großangelegten Cyberangriffs die Handlungssicherheit aller Beteiligten gewährleisten.

Handlungsfeld 3: Datenmanagement und Lagebilder

Hybride Bedrohungslagen erfordern eine abgestimmte Reaktion über Zuständigkeitsgrenzen hinweg. Dafür sind **ein gemeinsames Datenmanagement** und ein **integriertes Lagebild** mit abgestuften Zugriffsrechten für alle relevanten Akteure von Polizei, Feuerwehr und Verwaltungsstrukturen bis hin zu militärischen Stellen nötig. Ein solches Lagebild ist ein dynamischer Informationsverbund: kontextbezogen, rollenbasiert, aktuell. Heute entstehen Lagebilder oft mit inkompatiblen Systemen, pauschalen Zugriffsregeln, verzögerter Datenlage und uneinheitlicher Datenqualität: Einige Akteure nutzen präzise Geodaten und Echtzeitmeldungen, andere arbeiten mit groben Lagebeschreibungen, statischen Standardreports oder manuell aggregierten Informationen; eine gemeinsame Lagebeurteilung ist auf dieser Basis kaum möglich.

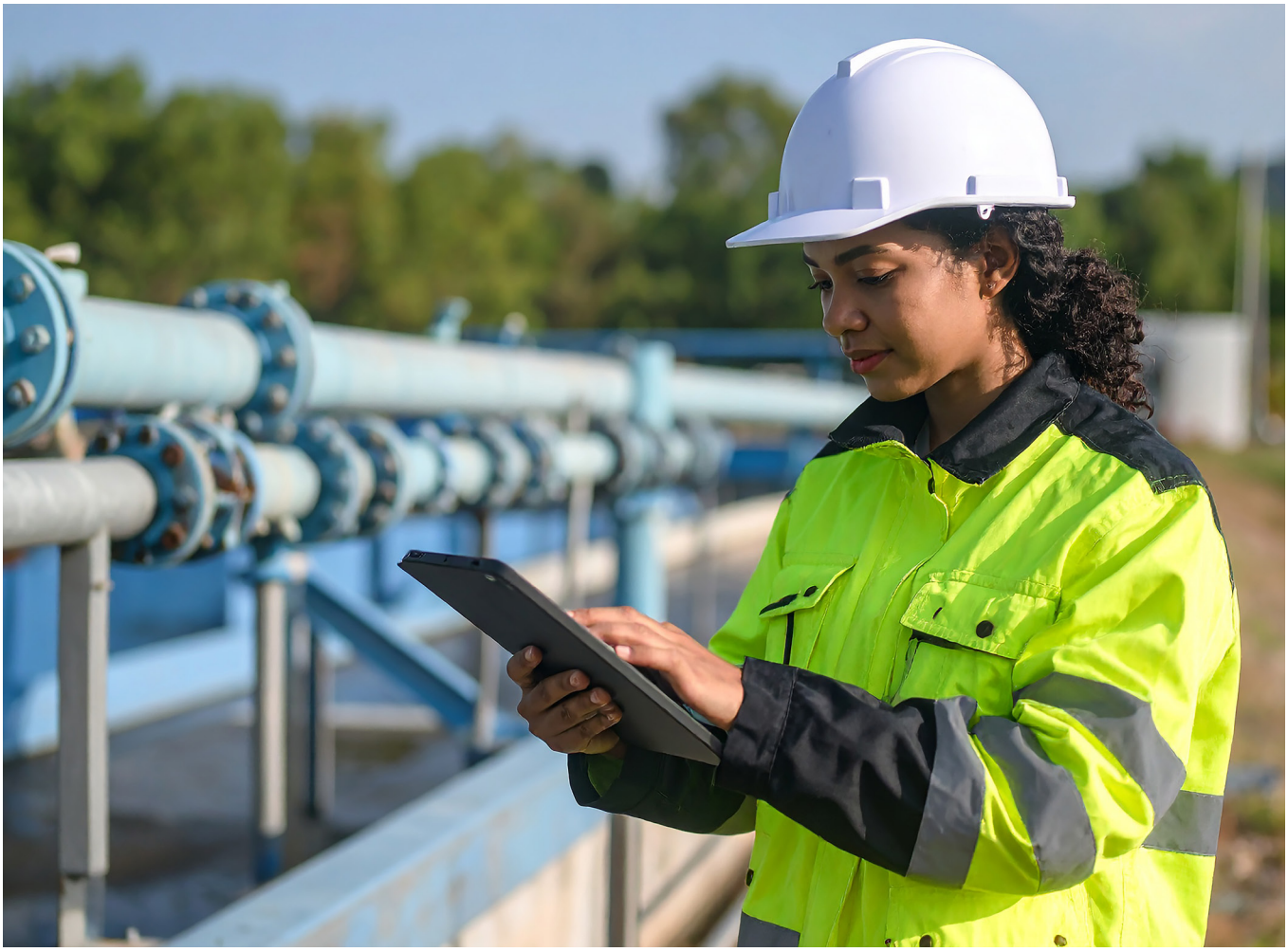
Ein zukunftsfähiges Lagebild für die ZMZ braucht deshalb **Verbundstrukturen** statt isolierter Zentralsysteme, **abgestufte, kontextbezogene Sichtbarkeit** sowie **Echtzeitdatenflüsse** zur lagegerechten und koordinierten Entscheidungsfindung.

Das **Maritime Sicherheitszentrum (MSZ)** in Cuxhaven zeigt, dass ressortübergreifende Lagearbeit im Alltag möglich ist. Bundes- und Landesbehörden arbeiten dort mit definierten Zugriffsrechten in einem gemeinsamen Lagebild – integriert, abgestimmt, einsatznah. Auch wenn dieses Modell nicht 1:1 auf alle ZMZ-Kontexte übertragbar ist, liefert es wertvolle Hinweise darauf, wie Struktur, Technik und Vertrauen im föderalen Raum erfolgreich verzahnt werden können.

Ein Beispiel etablierter Lagekoordination ist das **Gemeinsame Melde- und Lagezentrum (GMLZ)** im BBK. Es bündelt Informationen aus Bund, Ländern und Fachstellen – auch mit militärischer Einbindung im Wege der Amtshilfe. Zwar koordiniert das GMLZ zentrale Lagemeldungen, bietet aber kein dezentrales operatives Lagebild mit Echtzeitfähigkeit oder abgestuften Zugriffen. Für die ZMZ zeigt es: Verfahren funktionieren, aber Plattform und Führung fehlen. Nicht die Datenmenge entscheidet, sondern ihre Verfügbarkeit zur richtigen Zeit, im richtigen Kontext und bei den richtigen Akteuren. Ohne diese Grundlage bleibt Koordination im Ernstfall reaktiv statt strategisch geführt.

Handlungsfeld 4: Schutz kritischer Infrastrukturen – Resilienz durch regionale Sicherheitscluster stärken

Kritische Infrastrukturen (KRITIS) sichern Energie, Gesundheit, Kommunikation sowie Mobilität und sind in hybriden Bedrohungslagen bevorzugte Angriffsziele. Die Flutkatastrophe im Ahrtal 2021 hat gezeigt, wie rasch Versorgung, Kommunikation und Führung gleichzeitig versagen können. Ohne vorbereitete Strukturen, interoperable Systeme und klare Zuständigkeiten bleibt Resilienz eine Illusion. Mit dem KRITIS-Dachgesetz und dem NIS-2-Umsetzungsgesetz liegt ein verbindlicher Rahmen für sektorenübergreifende Schutzkonzepte vor. Daraus sind in der Fläche funktionierende Sicherheitscluster mit klaren Rollen, abgestimmter Technik und dauerhaft eingebundener Wirtschaft zu etablieren.



In einigen Bundesländern gibt es Ansätze für regionale Kooperationen zwischen KRITIS-Betreibern, Behörden, Polizei und Bundeswehr. Ziel ist, Schutzpläne gemeinsam zu entwickeln und regelmäßig zu testen. Doch diese Strukturen sind i. d. R. projektbezogen, ohne klare Führung oder technische Anbindung. Im Krisenfall fehlen verbindliche Abläufe und Rollen. Wirksamer KRITIS-Schutz im Verbund gelingt im Alltag aber nur durch konsequente Struktur und Verbindlichkeit sowie gelebte Zusammenarbeit, z. B. in Form regionaler Sicherheitscluster.

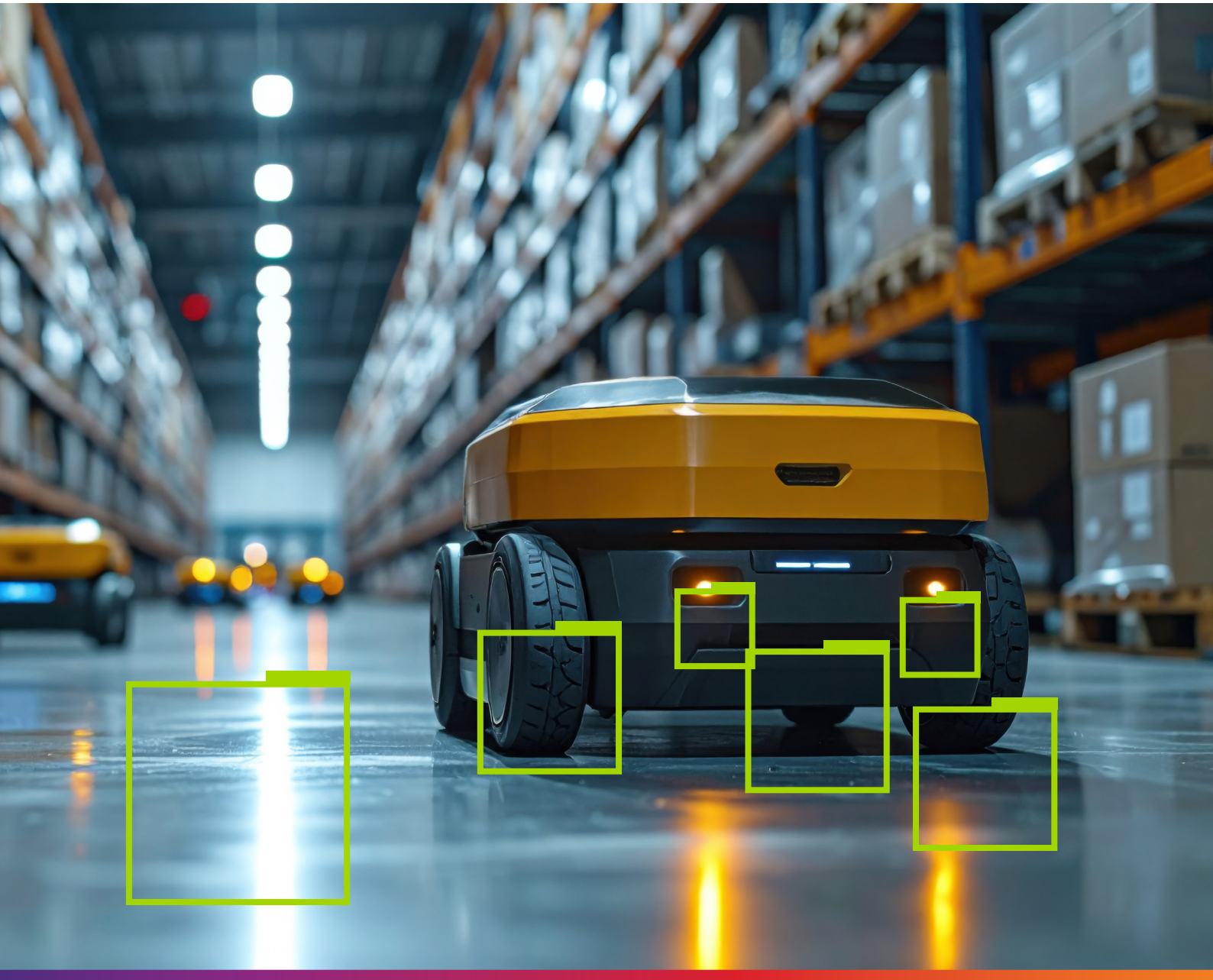
Handlungsfeld 5:
Logistik und Mobilität

BOS und Bundeswehr müssen ihre verteilten logistischen Standorte und Kapazitäten massiv weiterentwickeln, um komplexere Bevorratungs-, Bewirtschaftungs- und Maintenance-Anforderungen zu erfüllen. Dazu vier Beispiele:

Predictive-Digital-Twin-Ansätze zahlen auf die Planungs- und Integrationsfähigkeit ein, weil sie mithilfe von Simulations- und ML-Techniken die Verarbeitung der durch die virtuelle Abbildung physischer Objekte und Prozesse entstehenden Daten ermöglichen.

Performance-Based Logistics (PBL) entlastet BOS und Bundeswehr von Bevorratungs-, Bewirtschaftungs- und Maintenance-Aufgaben durch Übertragung auf externe Industrie-/DL-Partner: Kritische Erfolgsfaktoren sind eine vertragsverträgliche Bedarfsplanung, Einzugsgebietebildung und Standortbündelung.

Smarte **Warehouse-Management-Systeme (WMS)** steigern Geschwindigkeit und Effizienz der ZMZ durch standardisierte Logistikprozesse, Echtzeitdaten zu Artikelbeständen und Ressourcenauslastungen, automatisierte Materialflüsse sowie RFID-basierte Mess- und Steuerungssysteme. In Verbindung mit dem Einsatz von Logistikdrohnen kann zudem die Versorgungsleistung gesteigert werden. Im Rahmen der **datengetriebenen Logistik** zahlen Stammdatenkonsistenz, gemeinsam nutzbare artikel- und fähigkeitsbezogene Datenräume sowie geographische und Lifecycle-Management-basierte Analyse- und Simulationsmethoden auf die Planungsfähigkeit und den wirtschaftlichen Betrieb der künftig stärker verbundenen logistischen Systeme ein.



Fazit: Zivil-Militärische Zusammenarbeit

Angesichts zunehmend komplexerer und hybrider Bedrohungslagen erweist sich die Fähigkeit zum koordinierten, gesamtstaatlichen Handeln als Schlüsselfähigkeit. ZMZ steht dabei nicht länger für punktuelle Unterstützung, sondern für die strukturierte, dauerhafte, technologiegestützte Integration ziviler und militärischer Akteure.

ZMZ schafft gemeinsame Führungsstrukturen, plant mit Fokus auf aktuelle zivile und militärische Krisenszenarien, konsolidiert Lagebilder und verbindet operative Fähigkeiten, Ressourcen und Material über föderale Ebenen hinweg. Damit wird sie zum Rückgrat einer widerstandsfähigen Sicherheitsarchitektur sowohl in Friedenszeiten als auch im Krisen- und Verteidigungsfall. ZMZ ist weit mehr als ein Kooperationsinstrument, sie ist Ausdruck eines neuen Verständnisses von Sicherheit, das vernetzt, adaptiv und souverän ist. Wer Resilienz ernst nimmt, muss ZMZ strategisch denken, institutionell verankern und technologisch unterfüttern.

Ihre Ansprechpartner

Axel Lips, Client Unit Partner Defence
axel.lips@soprasteria.com

Thomas Kling, Client Unit Partner BKA
thomas.kling@soprasteria.com

Dr. Ganen Sethupathy, Client Unit Partner BOS
ganen.sethupathy@soprasteria.com

Stephan Koch, Senior Manager BOS
stephan.koch@soprasteria.com

Olaf Janßen, Head of Cyber Security
olaf.janssen@soprasteria.com

Kontakt:

Sopra Steria SE
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
T. 040 22703-0
E. info.de@soprasteria.com