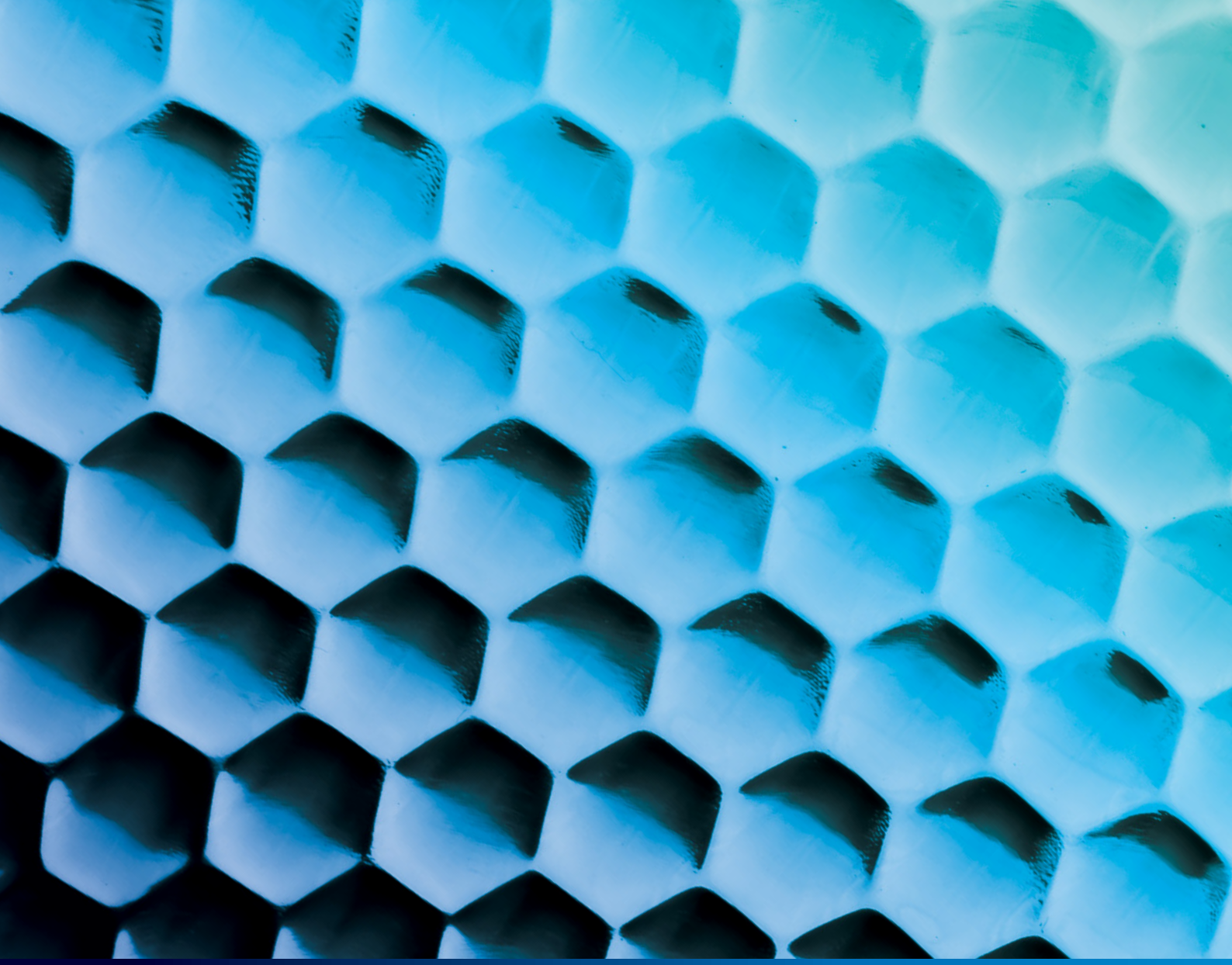
POINT OF VIEW

Gesamtverteidigung *Deutschland*

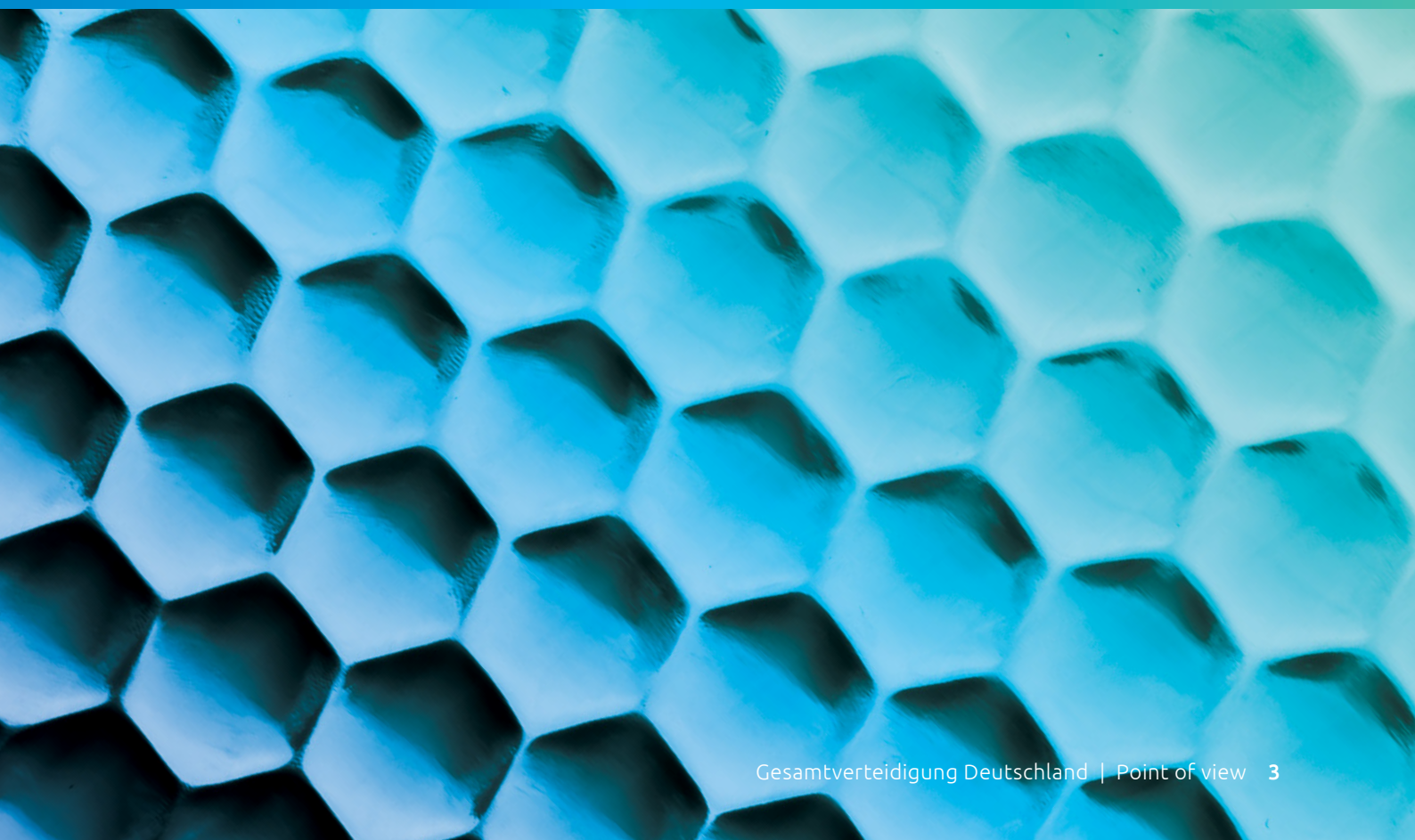
Capgemini



Quellen

1 SWR: Generalleutnant der Bundeswehr: Was passiert, wenn Deutschland angegriffen wird?
2 Deutschlandfunk: Russland, die NATO und die Kriegsgefahr
3 BfV: Gefährdungen durch russische Spionage, Sabotage und Desinformation
4 Tagesschau: NATO einigt sich auf Fünf-Prozent-Ziel
5 Spiegel: Nato-Chef Rutte fordert von Deutschland höhere Verteidigungsausgaben
6 ZDFheute: Merz' Wende in der Schuldenpolitik: Whatever it takes
7 Deutscher Landkreistag (DLT): Operationsplan und Zivilschutz: „Wir müssen vorbereitet sein"
8 Bundeswehr: Operationsplan Deutschland
9 BR24: Drehscheibe Deutschland: Worauf sich die Bundeswehr einstellt
10 Bundeswehr: „Nachgefragt" – Jetzt ist die Stunde der Europäer
11 BBK: Zivil-Militärische Zusammenarbeit im nationalen Bereich
12 BMI: Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien – (RRGV)
13 NATO: What is NATO?
14 BMVg: Das Bundesministerium der Verteidigung; und dort verlinkte Seiten
15 Bundeswehr: Die Organisation der Bundeswehr
16, 17 BMI: Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien – (RRGV)
18 BMI: Wer macht was beim Zivil- und Katastrophenschutz?
19, 20 BMI: Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien – (RRGV)
21 BBK: Host Nation Support in Deutschland
22 Fraunhofer: Verteidigungsforschung in der Zeitenwende
23 BBK: Zivil-Militärische Zusammenarbeit im nationalen Bereich
24 §§ 1 I Nr. 3, II, 3 II Nr. 3, Nr. 4, § 7 VerkLG
25 §§ 1, 7 MinÖlBewV
26 §§ 1 I S. 1 Nr. 1, Nr. 4 EnSiG
27 BMI: Stärkerer Schutz von kritischer Infrastruktur vor illegal fliegenden Drohnen
28 StMI Bayern: Schutz vor Drohnen: Ministerrat schafft klare Regeln im PAG und plant Drohnenkompetenzzentrum
29 BMI: Mehr Befugnisse für die Drohnenabwehr und den Schutz von Flughäfen
30 §§ 3 I Nr. 3, 4 a.E.: „Berücksichtigt wurde aber auch die Technisierung und Digitalisierung, indem Betreiber von Informations- und Kommunikationssystemen als Verkehrsunternehmen iSd VerkLG eingestuft wurden"
31 § 22 I Nr. 1 lit. c, Nr. 2 lit. c BDSG
32 Nature human behavior: A systematic review of worldwide causal and correlational evidence on digital media and democracy
33 BBK: Umfrage Bundesweiter Warntag 2025: 97 Prozent der Befragten erhalten Warnung

Inhaltsverzeichnis



01

Sicherheitspolitische *Ausgangslage*

Die militärische Eskalation in der Ukraine hat eine tiefgreifende Zäsur in der europäischen Sicherheitsordnung ausgelöst. Die Realität bewaffneter Auseinandersetzungen auf europäischem Boden, die massive Aufstockung von Streitkräften sowie die spannungsgeladene Beziehung zwischen der NATO und Russland führen zu einer hochriskanten Lage mit erheblichem Potenzial für weitere Zuspitzungen.

Diese Entwicklung wird durch eine zunehmend prekäre globale Wirtschaftslage verschärft, die sowohl die Widerstands- als auch die Verteidigungsfähigkeit Europas vor erhebliche Herausforderungen stellt. Eine glaubwürdige Abschreckung bleibt das zentrale Element zur Wahrung des Friedens. Sie erfordert militärische Stärke, eine widerstandsfähige Sicherheitsarchitektur und eine resiliente Zivilgesellschaft, um Bedrohungen aktiv zu begegnen und Krisen nachhaltig zu bewältigen.

„Russland will die NATO unterminieren, europäische Demokratien destabilisieren, unsere Gesellschaften spalten und einschüchtern."

Martin Jäger, *Präsident BND*

Hybride Bedrohungen gegen Deutschland

Der stellvertretende Befehlshaber des Operativen Führungskommandos der Bundeswehr und Kommandeur Territoriale Aufgaben, Generalleutnant André Bodemann, beschreibt die aktuelle Lage als *„eine Phase, in der wir zwar juristisch noch keinen Krieg haben, aber schon lange nicht mehr in Frieden leben, da wir täglich bedroht werden."*[1]

Zahlreiche feindliche Aktivitäten gegenüber der Bundesrepublik Deutschland sind bereits dokumentiert. Auch wenn nicht in jedem Fall zweifelsfrei nachgewiesen werden kann, von wem diese Angriffe ausgehen, sind sie dennoch immer ernst zu nehmen. Die Angriffe fokussieren sich dabei insbesondere auf [2, 3]:

ABBILDUNG 1:

Bedrohungslage

Cyberangriffe
auf staatliche Institutionen und Unternehmen

Desinformations-kampagnen
über Rundfunk und soziale Netzwerke

Spionageaktivitäten
darunter der Einsatz russischer Spionageschiffe in der Ostsee und Drohnen über Bw-Kasernen

Sabotageakte
gegen kritische Infrastrukturen, wie Bahnstrecken und Flughäfen

1 SWR: Generalleutnant der Bundeswehr: Was passiert, wenn Deutschland angegriffen wird?
2 Deutschlandfunk: Russland, die NATO und die Kriegsgefahr
3 BfV: Gefährdungen durch russische Spionage, Sabotage und Desinformation

Politische Reaktionen

Angesichts der zunehmenden Bedrohungslage wurde im Juni 2025 von allen 32 NATO-Mitgliedstaaten eine spürbare Erhöhung der Verteidigungsausgaben beschlossen.

Konkret wird das Ziel für die Verteidigungsausgaben auf insgesamt **5%** (3,5 % Verteidigungsausgaben 1,5 % sicherheitsrelevante Infrastruktur) des Bruttoinlandsprodukts bis spätestens 2035 angehoben.[4]

NATO-Generalssekretär Rutte wurde dabei deutlich: *„Wir müssen uns auf Krieg vorbereiten. Das ist der beste Weg, um Krieg zu vermeiden."*[5] Die sicherheitspolitische Zeitenwende erfordert daher finanzpolitischen Mut. Um strategische Handlungsfähigkeit zu sichern, verabschiedeten Bundestag und Bundesrat ein 500-Milliarden-Euro-Sondervermögen für Verteidigung und Infrastruktur. Kernpunkte sind eine Reform der Schuldenbremse, die teilweise Ausklammerung von Rüstungsausgaben sowie mehr finanzielle Spielräume für die Länder. Es ist ein Kurswechsel, weg von reiner Fiskaldisziplin, hin zu investiver Resilienz. Merz erläuterte diesbezüglich: *„Angesichts der Bedrohungen unserer Freiheit und des Friedens auf unserem Kontinent muss jetzt auch für unsere Verteidigung gelten: Whatever it takes."*[6]

Um der Komplexität dieser Bedrohungslage gerecht zu werden, sind Effizienz und Pragmatismus in sicherheitspolitischen Entscheidungsprozessen unerlässlich. Mit innovativen, datengetriebenen Lösungen unterstützt Capgemini die Optimierung von Entscheidungsprozessen, die Stärkung der Resilienz von Infrastrukturen und die Entwicklung von Strategien, die sowohl kurzfristig Orientierung bieten als auch langfristig nachhaltig sind. In Zeiten dynamischer geopolitischer Herausforderungen tragen wir damit zur Stärkung der gesamtstaatlichen Verteidigungsfähigkeit bei.

4 Tagesschau: NATO einigt sich auf Fünf-Prozent-Ziel

5 Spiegel: Nato-Chef Rutte fordert von Deutschland höhere Verteidigungsausgaben

6 ZDFheute: Merz' Wende in der Schuldenpolitik: Whatever it takes

Gesamtstaatliche Verteidigung Deutschlands

im Kontext

Deutschland muss im Verteidigungsfall gesamtstaatlich verteidigt werden, wobei staatliche Institutionen, militärischeStrukturen und zivilgesellschaftliche Akteure nahtlos zusammenwirken müssen.

In diesem neuen sicherheitspolitischen Kontext stellt sich die Frage:

Wer übernimmt welche Aufgaben im Spannungs- und Verteidigungsfall? Welche Rolle spielen militärische Kräfte, welche die zivilen – und wie können diese beiden Bereiche effektiv und effizient miteinander verzahnt werden?

Während es im Operationsplan Deutschland bereits klare Rollen und Strategien für den militärischen Anteil der Verteidigung gibt, ist der zivile Beitrag zur Verteidigungsfähigkeit Deutschlands noch nicht in allen Bereichen strategisch durchdacht. **Ein spezifischer „Operationsplan Zivilverteidigung“ [7] ist erforderlich.**

ABBILDUNG 2:

Schema Gesamtverteidigung Deutschlands

7 Deutscher Landkreistag (DLT): Operationsplan und Zivilschutz: „Wir müssen vorbereitet sein“

Operationsplan Deutschland

Der Operationsplan Deutschland (OPLAN DEU) ist ein strategisches Instrument, das primär den militärischen Anteil der Landes- und Bündnisverteidigung (LV/BV) regelt und klare Handlungsanweisungen für den Ernstfall liefert.

Der als geheim eingestufte Operationsplan legt fest, welche Ressourcen mobilisiert werden, welche Akteure koordiniert und welche Maßnahmen ergriffen werden müssen, um die Anforderungen der NATO-Verteidigungspläne zu erfüllen und gleichzeitig die Sicherheit sowie Funktionsfähigkeit des deutschen Staates zu gewährleisten.[8]

Als bevölkerungsreichstes und wirtschaftlich stärkstes Land in Zentraleuropa fungiert Deutschland zudem als logistische Drehscheibe für den Aufmarsch alliierter NATO-Kräfte im Fall der Bündnisverteidigung an der Ostflanke.[9] Dies erfordert nicht nur die Sicherung von Transportwegen und kritischer Infrastruktur, sondern auch die effektive Koordination zwischen militärischen und zivilen Akteuren – von staatlichen Behörden über private Dienstleister bis hin zu zivilgesellschaftlichen Strukturen.

Der Operationsplan definiert daher nicht ausschließlich militärische Maßnahmen, sondern berücksichtigt auch die Resilienz kritischer Infrastrukturen – von der Energie- und Lebensmittelversorgung bis hin zu Transport- und Kommunikationsnetzen. Die Maßnahmen im Rahmen des Operationsplans erfüll neben ihrer operativen auch eine präventive Funktion. Durch glaubwürdige Abschreckung, basierend auf militärischer Stärke und einer hohen gesamtstaatlichen Reaktionsfähigkeit, soll das Risiko eines militärischen Konflikts minimiert werden.[10]

8 Bundeswehr: Operationsplan Deutschland
9 BR24: Drehscheibe Deutschland: Worauf sich die Bundeswehr einstellt
10 Bundeswehr: „Nachgefragt“ – Jetzt ist die Stunde der Europäer

Zivil-Militärische Zusammenarbeit

Die Gesamtverteidigung teilt sich in einen militärischen und einen zivilen Anteil auf. In der Zeitenwende kann sich der Blick deshalb nicht allein auf die militärische Seite der Verteidigung richten.

Denn auch die Menschen in den Unternehmen, Verwaltungen oder zivilen Einsatzorganisationen leisten im Ernstfall einen unverzichtbaren Beitrag für die Sicherheit der Menschen in Deutschland. Die Zivil-Militärische Zusammenarbeit (ZMZ) ist ein integraler Bestandteil einer erfolgreichen Verteidigungsstrategie. Verteidigung kann in Deutschland nur gesamtstaatlich gedacht werden – sie ist nicht allein Aufgabe der Bundeswehr. Zwar darf die Bundeswehr gemäß Artikel 35 des Grundgesetzes (GG) in Katastrophenfällen Amtshilfe leisten, ihre primäre Verantwortung liegt jedoch in der Landes- und Bündnisverteidigung. Die Rolle des zivilen Sektors in der Gesamtverteidigung ist daher nicht nur ergänzend, sondern unverzichtbar. Eine starke gesamtstaatliche Resilienz ist erreichbar, wenn jeder Akteur seine Verantwortung erkennt und wahrnimmt. Die Bundeswehr kann sich dadurch auf ihre Kernaufgabe der militärischen Landes- und Bündnisverteidigung konzentrieren, während die nicht-militärischen Akteure die Hauptverantwortung für die folgenden vier Grundpfeiler der zivilen Verteidigung tragen:

- Aufrechterhaltung der Staats- und Regierungsfunktionen
- Zivilschutz
- Versorgung der Bevölkerung
- Unterstützung der Streitkräfte[11]

„Die militärische und die zivile Verteidigung sind zwei Seiten derselben Medaille namens Gesamtverteidigung. In der Zeitenwende kann sich der Blick deshalb nicht allein auf die militärische Seite der Verteidigung richten."

Leon Eckert, *MdB*

An der zivil-militärischen Schnittstelle setzt Capgemini an. Mit langjähriger Erfahrung als Technologiepartner in der Zusammenarbeit mit öffentlichen und privaten Akteuren ist Capgemini ein Bindeglied zwischen Ressorts und Organisationen – mit dem Ziel, komplexe Stakeholderlandschaften zu orchestrieren und gemeinsame Lösungen in anspruchsvollen Kontexten voranzutreiben. Capgemini möchte als werteorientiertes Unternehmen europäischen Ursprungs einen pragmatischen Beitrag zur Stärkung der zivil-militärischen Zusammenarbeit sowie zu einem „Zivilen Operationsplan" leisten.

ABBILDUNG 3:

Capgemini als Bindeglied und Treiber

11 BBK: Zivil-Militärische Zusammenarbeit im nationalen Bereich

03

Akteure in der Gesamtverteidigung

Zunächst wird jedoch definiert, welche militärischen und zivilen Akteure zur Gewährleistung der Gesamtverteidigung Deutschlands eng verzahnt zusammenarbeiten müssen und welche Rollen sie in der LV/BV übernehmen.

Die Rahmenrichtlinien für die Gesamtverteidigung (RRGV) gliedern diese in die Ebenen Politische Führung und Staat, Bundeswehr und militärische Strukturen, Zivile Verteidigung und Behörden sowie Wirtschaft und Gesellschaft[12], welche sich in drei Hauptgruppen zusammenfassen lassen: **militärische, zivile und wirtschaftliche Akteure**.

Der neu gegründete Nationale Sicherheitsrat (NSR) nimmt seine Arbeit als strategisches Steuerungsgremium der Akteursgruppen unserer Gesamtverteidigung am 1. Januar 2026 auf.

Er wird ressortübergreifend die Bereiche innere, äußere, wirtschaftliche und digitale Sicherheit sowie zivile und militärische Verteidigung koordinieren.

Als zentrale Plattform für Lagebewertung, strategische Vorausschau und Krisenkoordination stärkt er die Handlungsfähigkeit des Staates. **Damit wird er zum Herzstück unserer Akteure für Resilienz und Verteidigungsfähigkeit.**

Der Rat ersetzt den Bundessicherheitsrat und bündelt sicherheitsrelevante Entscheidungen unter Leitung des Bundeskanzlers.

ABBILDUNG 4:

Akteure Gesamtverteidigung

12 BMI: Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien – (RRGV)

Militärische Akteure

Den militärischen Block bilden auf internationaler Ebene die NATO, auf nationaler Ebene das Bundesministerium der Verteidigung (BMVg) bzw. die nachgeordneten Bereiche.

Die NATO ist ein transatlantisches Verteidigungsbündnis, das durch kollektive Verteidigungsmaßnahmen die Territorien seiner 32 nordamerikanischen und europäischen Mitgliedstaaten absichert und dadurch potenzielle Aggressoren abschreckt. Sie koordiniert im Bündnisverteidigungsfall Truppenbewegungen auf internationaler Ebene und schafft einen gemeinsamen Handlungsrahmen.[13]

Das Bundesministerium der Verteidigung (BMVg) ist die oberste Bundesbehörde für alle militärischen und sicherheitsrelevanten Aufgaben des Bundes. Es legt die Rahmenbedingungen für die militärische Planung fest, koordiniert Einsätze der Streitkräfte und stellt sicher, dass die Verteidigungsfähigkeit Deutschlands im Einklang mit den NATO-Verpflichtungen steht.[14]

Die Bundeswehr teilt sich in die Streitkräfteund die Wehrverwaltung auf. Die Streitkräfte unterteilen sich wiederum in die Teilstreitkräfte Heer, Luftwaffe, Marine und Cyber sowie den Unterstützungsbereich. Ihr Kernauftrag liegt in der Landes- und Bündnisverteidigung.[15] Darüberhinaus übernimmt sie Aufgaben in internationalen Missionen der NATO, der EU oder der UN sowie im Rahmen der Amtshilfe bei Katastrophen und Krisenlagen im Inland.

Trotz dieser breiten Einsatzbereiche bleibt der Schutz der territorialen Integrität Deutschlands und die Verteidigung des Bündnisgebiets ihre vorrangige Aufgabe. Die Bundeswehr verfügt zudem über ein föderal ausgerichtetes Territoriales Netzwerk zur Unterstützung der zivilen und militärischen Verteidigung.[16]

13 NATO: What is NATO?

14 BMVg: Das Bundesministerium der Verteidigung; und dort verlinkte Seiten

15 Bundeswehr: Die Organisation der Bundeswehr

16 BMI: Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien – (RRGV)

Zivile Akteure

Landesverteidigung als holistischer Ansatz erfordert das Mitwirken zivilhoheitlicher Akteure. Das Bundesministerium des Innern (BMI) übernimmt hierbei eine zentrale Rolle, da es für innere Sicherheit, Bevölkerungsschutz und Cyberabwehr verantwortlich ist.

Es koordiniert Maßnahmen zwischen Bund, Ländern und Kommunen. Nachgeordnet ist das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Risikoanalysen erstellt, Katastrophenschutzmaßnahmen koordiniert und Warnsysteme, z. B. die Warn-App NINA, für die Bevölkerung betreibt.

Bund und Länder müssen in Krisensituationen die kontinuierliche Handlungsfähigkeit von Gesetzgebung, Regierung, Verwaltung und Rechtsprechung sicherstellen. Dazu gehört eine effiziente Zusammenarbeit, um gesetzliche Grundlagen bei Bedarf schnell anzupassen und Verfahren sowie Verwaltungsprozesse beschleunigt umzusetzen. Zur Abstimmung zwischen Bund und Ländern existieren Gremien wie die Innenministerkonferenz (IMK), der Arbeitskreis V (AK V) sowie der Bund-Länder-Krisenstab. Die Bundespolizei (BPol) übernimmt eine wichtige Rolle bei der Aufrechterhaltung der inneren Sicherheit, dem Schutz kritischer Infrastrukturen, der Terrorismusbekämpfung sowie der Sicherung von Verkehrswegen und Grenzschutz. Die Verfassungsorgane des Bundes und die Bundesministerien werden durch die BPol vor Gefahren geschützt. Darüber hinaus kann die BPol im Verteidigungsfall unter den Voraussetzungen des GG die Bundespolizei im gesamten Gebiet der Bundesrepublik Deutschland einsetzen.[17] Sie entlastet damit die Bundeswehr, die sich auf ihre militärischen Kernaufgaben konzentrieren kann. Ergänzend übernehmen die Polizeibehörden der Länder Aufgaben in der Gefahrenabwehr und im Katastrophenschutz, insbesondere bei regionalen Bedrohungslagen.[18]

Das Technische Hilfswerk (THW) ist die **„operative Einsatzorganisation des Bundes“** und leistet Unterstützung durch technische Hilfe, z. B. bei Evakuierungen, Instandsetzung von Infrastruktur und Bergungsarbeiten. Organisationen wie das Deutsche Rote Kreuz (DRK) sowie anerkannte Hilfsorganisationen wie Johanniter und Malteser unterstützen in Sanitätsdiensten, bei Evakuierungen und durch medizinische Versorgung.[19]

17 BMI: Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien – (RRGV)

18 BMI: Wer macht was beim Zivil- und Katastrophenschutz?

19 BMI: Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien – (RRGV)

Wirtschaftliche Akteure

Die Versorgung mit Lebensmitteln, Wasser und Energie muss für das Überleben und die Funktionsfähigkeit der Gesellschaft jederzeit gewährleistet sein. Versorgungsunternehmen und die Lebensmittelindustrie tragen die Verantwortung für stabile Lieferketten, effiziente Lagerhaltung und den Aufbau von Notfallreserven.

Dies umfasst auch Logistikdienstleister, die für den Transport lebenswichtiger Güter zuständig sind Energieversorger sind für die Bereitstellung von Strom und Treibstoff sowie für die Stabilität der Netzinfrastruktur verantwortlich – unerlässliche Grundvoraussetzungen für militärische Operationen und zivile Funktionen. Ohne eine gesicherte Energieversorgung sind beispielsweise groß angelegte Truppenbewegungen, der Erhalt der Kommunikationswege oder der Funktionsfähigkeit kritischer Infrastrukturen nicht möglich.

Als **„Host Nation Support (kurz: HNS)“** bezeichnet man in der NATO die zivile und militärische Unterstützung alliierter, ausländischer Streitkräfte in einem Gastland durch dessen Regierung.[21]

Obwohl die Bundeswehr über eigene logistische Fähigkeiten verfügt, ist sie im Verteidigungsfall auf die Unterstützung durch Logistik- und Transportunternehmen angewiesen, um der Rolle Deutschlands als logistische Drehscheibe für NATO-Operationen gerecht zu werden, u. a. im Rahmen des Host Nation Support. Zivile Logistikunternehmen leisten ihren Beitrag durch Transportmanagement, Routenplanung, Materialversorgung und Infrastrukturunterstützung.

Dazu gehören Unternehmen des Schienenverkehrs, der Luftfahrt, des Straßentransports sowie Hafen- und Flughafenbetreiber.[20] Telekommunikationsunternehmen stellen Kommunikationsnetze, Notfallverbindungen und Cyber-Sicherheitsstrukturen bereit. Die Sicherstellung der Netzstabilität, insbesondere in Krisenzeiten, ist ein wesentlicher Bestandteil der nationalen Verteidigungsplanung. Hier sind auch die Inhouse-Gesellschaften des Bundes in der Pflicht und müssen, wie beispielsweise das IT-Systemhaus der Bundeswehr (BWI), die Aufrechterhaltung und Resilienz sicherstellen. IT- und Cybersicherheitsunternehmen spielen eine Schlüsselrolle beim Schutz von Netzwerken, der Abwehr von Cyberangriffen und der Sicherung digitaler Infrastrukturen.[22]

Schließlich sind auch die Unternehmen der Pharmaindustrie und des Gesundheitswesens unverzichtbar. Sie gewährleisten die medizinische Versorgung, insbesondere bei Großschadensereignissen, durch die Produktion von Arzneimitteln, den Betrieb von Krankenhäusern und die Unterstützung des zivilen Sanitätsdienstes.

Es bedarf nun innovativer Ideen, um die Gesamtverteidigung Deutschlands gemeinsam mit allen Beteiligten sicherzustellen. Rollen und Aufgaben müssen klar definiert werden und gezielt auf spezifische Bedrohungsszenarien vorbereiten. Zudem braucht es digitale Lösungen, um Kommunikation und Kollaboration zu verbessern.

20 BMI: Rahmenrichtlinien für die Gesamtverteidigung – Gesamtverteidigungsrichtlinien – (RRGV)

21 BBK: Host Nation Support in Deutschland

22 Fraunhofer: Verteidigungsforschung in der Zeitenwende

Herausforderungen und *Lösungen*

04

Capgemini hat sich daher vier Herausforderungen im Rahmen der Gesamtverteidigung herausgegriffen, für die es ein konkretes Lösungsangebot – strategisch, organisatorisch oder technologisch – macht. Wir bringen ein breites Fähigkeitenportfolio ein, dass bei der Stärkung der zivil-militärischen Zusammenarbeit einen Unterschied macht, sei es Ressourcenmanagement, Datenanalyse, Organisationsentwicklung, Stakeholdermanagement oder Kommunikation. Zudem basieren die Lösungsansätze auf unserer langjährigen Domänenexpertise, die wir bei zahlreichen Kunden aus dem privaten und öffentlichen Sektor gesammelt haben.

1. Zivile Unterstützung und Resilienz

Herausforderung: Konkurrierende Bedarfe

Im Ernstfall der Landes- und Bündnisverteidigung ist die Verteilung knapper Ressourcen von konkurrierenden Bedarfen geprägt. Dabei muss strategisch abgewogen werden, welche Akteure in welchen Situationen prioritär Zugang zu lebenswichtigen logistischen, administrativen und infrastrukturellen Ressourcen erhalten. Deutschland steht im Spannungsfall in der Verantwortung, als Host Nation Support alliierte Streitkräfte bei ihrer Stationierung, im Transit und bei militärischen Operationen auf deutschem Territorium zu unterstützen.[23] Knappe Ressourcen wie Unterkünfte, Treibstoff, medizinische Versorgung und Kommunikationsnetze müssen zwischen militärischen und zivilen Bedarfen priorisiert werden.

Dies führt zu Zielkonflikten, wenn beispielsweise Hotels oder Wohnhäuser für alliierte Streitkräfte reserviert werden, während diese gleichzeitig für die Unterbringung von Geflüchteten benötigt werden. Auch Sporthallen, die als Notunterkünfte dienen, könntenmilitärischen Anforderungen weichen. Die Verfügbarkeit von Treibstoff ist ein weiteres kritisches Beispiel: Treibstoff, der für militärische Transporte vorgesehen ist, könnte die Betriebsfähigkeit des privaten Transportgewerbes beeinträchtigen und zu Einschränkungen im individuellen und öffentlichen Nah- und Fernverkehr führen.

Aktuell ist die Datenlandschaft in Bezug auf durch die Streitkräfte nutzbare zivile Ressourcen in Deutschland unübersichtlich und geprägt von mangelnder Integration – Faktoren, die im Ernstfall zu gravierenden Koordinationsproblemen und einem potenziellen Kollaps der operativen Steuerung führen könnten.

Im Bedarfsfall wären **grundlegende Informationen** wie die Anzahl verfügbarer ziviler Unterstützungskräfte, Krankenhauskapazitäten oder logistische Ressourcen nur schwer beschaffbar.

23 BBK: Zivil-Militärische Zusammenarbeit im nationalen Bereich

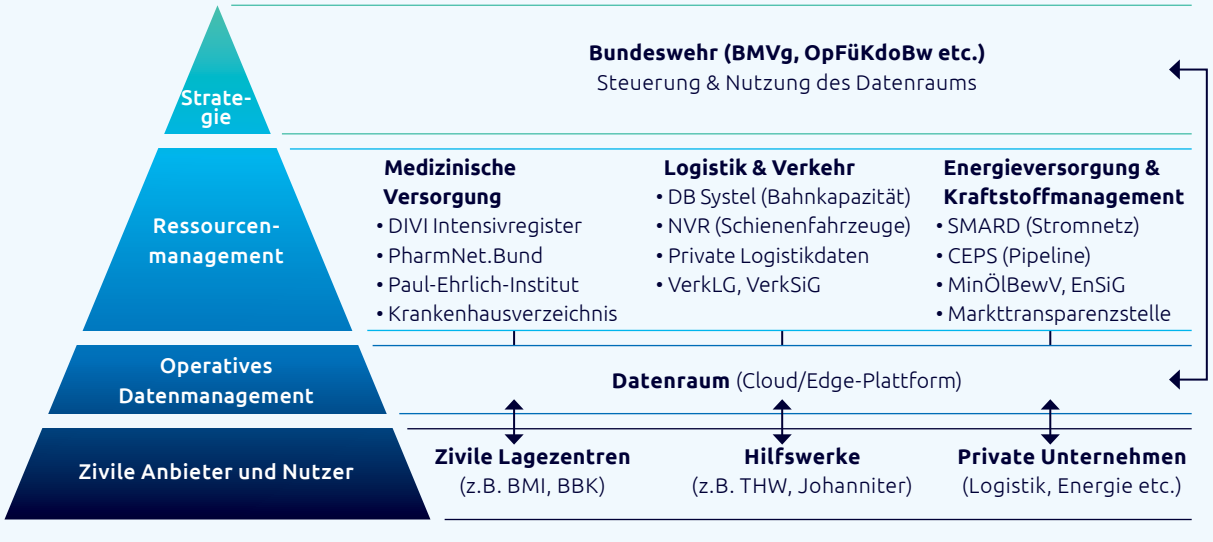
Lösung: Datenraum für das zivil-militärische Ressourcenmanagement

Capgemini regt daher den Aufbau eines gemeinsamen Datenraumes an, der diese Ressourcen heute sichtbar und bereits im Vorfeld steuerbar macht, um im Ernstfall effizient und koordiniert agieren zu können. Neben dem strategischen Aufbau von Ressourcen und der Erfüllung von Bedarfen bereits vor dem Ernstfall können die Daten zudem auch in zivilen Lagezentren wie beim BMI genutzt werden und stärken über den gemeinsamen Datenraum zudem die Kooperation und den Austausch mit zivilen Akteuren. Eine Vielzahl an relevanten Daten zu nutzbaren zivilen Ressourcen ist dabei öffentlich einsehbar. Daten, die einer Zugangsbeschränkung unterliegen, können unter Berufung auf bestehende rechtliche Grundlagen durch Bundesbehörden oder einen Kauf von Daten zugänglich gemacht werden.

Wir fokussieren uns in diesem Dokument dabei auf die Themencluster der medizinischen Versorgung, Logistik und Energieversorgung, um eine Indikation zur Machbarkeit eines zivil-militärischen Datenraums zu bieten und eine Diskussionsgrundlage für dessen Aufbau zu schaffen.

ABBILDUNG 5:

Architekturskizze Datenraum Ressourcenmanagement



Gesundheitswesen & Medizinische Versorgung

Ein leistungsfähiges Gesundheitswesen ist im Krisenfall unverzichtbar, um die medizinische Versorgung von Zivilisten, militärischem Personal und möglichen Flüchtlingsströmen sicherzustellen. Besonders in Verteidigungsszenarien besteht die Gefahr einer schnellen Überlastung der medizinischen Infrastruktur, weshalb eine vorausschauende Planung, gezielte Steuerung und kontinuierliche Überwachung der verfügbaren Kapazitäten unerlässlich sind.

Der Zugriff auf die benötigten Daten ist auch bereits zu Friedenszeiten durch öffentlich zugängliche Daten gegeben. Das Krankenhausverzeichnis stellt beispielsweise Daten zu den Kapazitäten und Kompetenzen der deutschen Krankenhäuser zur Verfügung. Um auf eine tagesaktuelle Übersicht an verfügbaren Intensivbetten zuzugreifen, kann zudem das öffentlich einsehbare DIVI Intensivregister herangezogen werden.

Die Datenbank PharmNet.Bund wiederum verfügt über eine Vorratsaktualisierung der medizinischen Medikamenten- und Arzneimittelversorgung. Zu dieser haben Bundesbehörden wie das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) bereits heute einen Zugang. Die Bedarfsdeckung an Blutkonserven wird wöchentlich und öffentlich durch das Paul-Ehrlich-Institut gepflegt.

Durch die systematische Anbindung und Nutzung dieser zivilen Datenquellen sowie die Integration der vom Kommando Gesundheitsversorgung der Bundeswehr (KdoGesVersBw) gepflegten Daten zu medizinischen Einrichtungen kann die medizinische Versorgung zeitnah effizient gesteuert und überwacht werden. Dies trägt nicht nur zur Sicherstellung der medizinischen Versorgung in Notlagen bei, sondern verbessert auch die langfristige Resilienz des Gesundheitssystems.

Logistik & Verkehr

Im Bereich Logistik und Verkehr liegt der Fokus exemplarisch auf dem Transport auf dem Landweg; die folgenden Ansätze lassen sich aber auf Luft- und Schifffahrt übertragen. In Krisensituationen besteht ein hoher Bedarf an Logistikkapazitäten für militärische Zwecke, während gleichzeitig das zivile Leben so wenigwie möglich beeinflusst werden soll. Zur optimierten logistischen Planung von Material und Lebensmitteln wird ein Verzeichnis von verfügbaren Lagern sowie nutzbaren Logistikflotten daher als sinnvoll erachtet.

Zur optimalen Koordinierung von Kapazitäten kann ggf. auf Daten von DB Systel zur Auslastung und Kapazität des Bahnstreckennetzes zugegriffen werden. Ein entsprechender Zugang ist kommerziell erhältlich. Hinsichtlich der zugelassenen Schienenfahrzeuge ist es mit einem beantragten Zugang möglich, auf Daten des Nationalen Fahrzeugeinstellungsregisters (NVR) des Eisenbahn-Bundesamtes, in dem alle Schienenfahrzeuge registriert werden müssen, zuzugreifen. Über weitere kommerzielle Anbieter aus Deutschland sind auch Informationen zum rollenden Material anderer EU-Staaten verfügbar.

Mögliche Daten zu Logistikkapazitäten auf der Straße könnten private Paket- und Logistikunternehmen bereitstellen. Rechtliche Eingriffsmöglichkeiten hierzu bieten die bundesrechtlichen Versorgegesetze, insbesondere das Verkehrssicherstellungs- (VerkSiG) und das Verkehrsleistungsgesetz (VerkLG). Im Verteidigungsfall können sogenannte Nebenleistungen (Betrieb von Umschlaganlagen, Speditionsleistungen und Lagerei) von Speditionen und Lagerunternehmen angefordert werden.[24]

Außerhalb des Verteidigungsfalls wird vorgeschlagen, Anreize für Unternehmen zu schaffen, indem bei der Neuausschreibung von Logistikdienstleistungen für die Bundeswehr die Datenmitteilung zur Bedingung von zukünftigen Rahmenverträgen gemacht wird.

Mithilfe dieser Daten erhält die Bundeswehr einen Überblick über verfügbare Logistikkapazitäten, um im Bedarfsfall den Transport von Personal und Material zu koordinieren und strategische Kapazitäten aufzubauen.

24 §§ 1 I Nr. 3, II, 3 II Nr. 3, Nr. 4, § 7 VerkLG (Entscheidung durch Bundesministerium oder Bundesregierung zur Anwendung nötig)

Energie- & Kraftstoffversorgung

Die sichere Versorgung mit Energie und Kraftstoffen ist eine essenzielle Grundlage für die militärische Einsatzfähigkeit und die Aufrechterhaltung kritischer ziviler Infrastrukturen, sowohl in Krisenzeiten als auch im regulären Betrieb. Daher ist es erforderlich, jederzeit einen aktuellen Überblick über relevante Versorgungsstrukturen zu haben, um frühzeitig notwendige Maßnahmen einleiten zu können.

Es ist bereits heute möglich, über SMARD, einem Service der Bundesnetzagentur, die Nennleistung sowie die tagesaktuelle Leistung von deutschen Kraftwerken öffentlich abzurufen. Im Falle von Netzwerkproblemen kann auf diese Daten weitgehend auch über Langwellenempfänger für die Funkrundsteuerung zugegriffen werden.

Das mitteleuropäische Pipelinesystem (CEPS)ist für die Analyse der militärischen Kraftstoffversorgung der NATO bereits implementiert, kann jedoch um einen Zugang zu Daten der Füllstände an Tankstellen erweitert werden. Dieser Einblick wird derzeit nicht öffentlichgeteilt. Einen Eingriff in die unternehmensinternen Daten von Tankstellenbetreibern ermöglicht jedoch die Mineralölbewirtschaftungs-Verordnung (MinÖlBewV).[25] Darüber hinaus benennt das Energiesicherungsgesetz (EnSiG) eine Möglichkeit der Errichtung einer digitalen Plattform zur Maßnahmenumsetzung.[26]

Technisch lässt sich dabei, falls nötig, die bereits heute vorhandene Anbindung der Marktteilnehmer an die Markttransparenzstelle nutzen.

Die Nutzung dieser Datenquellen ermöglicht eine präzise Überwachung und Steuerung der Energie- und Kraftstoffversorgung, wodurch Engpässe frühzeitig erkannt, strategische Reserven effizient verwaltet und die Einsatzbereitschaft der Streitkräfte sowie die Stabilität kritischer Infrastrukturen sichergestellt werden können.

25 §§ 1, 7 MinÖlBewV

26 §§ 1 I S. 1 Nr. 1, Nr. 4 EnSiG

Weiteres

Im Krisenfall ist neben der Verfügbarkeit von Reservisten der Bundeswehr auch die Verfügbarkeit von zivilem Personal aus z. B. Polizei, Feuerwehren und dem Technischen Hilfswerk relevant. Wichtige Personalkapazitäten werden bereits durch das Gemeinsame Melde- und Lagezentrum von Bund und Ländern (GMLZ) gesammelt und können entsprechend nutzbar gemacht werden.

Zur Unterstützung von Verlegungen durch Deutschland ist es zudem sinnvoll, Daten über Unterkunfts-möglichkeiten zu erfassen. Hier sind öffentliche Hotel- und Ferienwohnungsportale sowie das Deutsche Jugendherbergswerk (DJH) leicht und zeitnah zu erschließende Datenquellen, welche den Aufbau und Betrieb von Rast- und Sammelräumen entlang von Marschrouten flankieren.

Daten zur Abdeckung und Funktionalität des deutschen Telekommunikationsnetzes sind über das Geoportal des Bundesamts für Kartographie und Geodäsie öffentlich zugänglich und können durch zusätzliche von der Bundesnetzagentur und Telekommunikationsunternehmen bereitgestellte Daten erweitert werden.

Der Datenraum zur zivil-militärischen Ressourcenplanung stellt einen **entscheidenden Baustein zur Nutzung ziviler Ressourcen in Krisensituationen** dar. Durch die Bündelung und Bereitstellung relevanter Daten für die Bundeswehr sowie, in zweiter Reihe, auch zivile Akteure können Engpässe frühzeitig erkannt, Ressourcen effizient gesteuert und Vorbereitungen gezielt getroffen werden.

2. Schutz und Sicherung verteidigungs-relevanter Infrastruktur

Herausforderung: Drohnenangriffe auf kritische Infrastruktur

Die wachsende Bedrohung kritischer Infrastrukturen und von Kasernen durch Drohnen stellt eine ernste Herausforderung dar. Das Bundesinnenministerium betont: *„Wir müssen unsere kritischen Infrastrukturen besser vor illegal fliegenden Drohnen schützen."*[27]

Energie- und Wasserversorgung, Verkehrs- und Industrieanlagen sowie Regierungsgebäude sind potenzielle Ziele für Spionage, Sabotage oder Angriffe. Besonders im Kontext hybrider Bedrohungen setzen staatliche und nichtstaatliche Akteure vermehrt Drohnen ein, um Cyberangriffe, Störungen in Versorgungsketten oder Destabilisierungsmaßnahmen durchzuführen. Zudem fehlt eine enge Zusammenarbeit zwischen zivilen und militärischen Akteuren. Unterschiedliche Zuständigkeiten auf Bundes- und Landesebene und fehlende Einsatzkonzepte erschweren eine effektive Reaktion auf Drohnenbedrohungen. Landespolizeien, die für Fälle von Spionage und Sabotage zuständig sind, verfügen z. B. oft (noch) nicht über die Fähigkeiten und Kapazitäten, militärisch eingesetzte Drohnen erfolgreich abzuwehren. Die Verfügbarkeit kommerzieller Drohnen mit fortschrittlicher Technologie verstärkt das Problem.

Von ISR-Drohnen (Intelligence, Surveillance, Reconnaissance) bis hin zu FPV-Drohnen mit Sprengladungen – moderne Systeme ermöglichen Angriffe auf kritische Infrastrukturen.

27 BMI: Stärkerer Schutz von kritischer Infrastruktur vor illegal fliegenden Drohnen

Lösung: Konzept zur zivil-militärischen Drohnenabwehr für kritische Infrastruktur

Als Technologiehaus, das in komplexer Problemlösung erfahren ist, unterstützt Capgemini ein umfassendes Konzept für die zivil-militärische Drohnenabwehr für kritische Infrastrukturen, das nicht nur technische Fähigkeiten, sondern auch organisatorische und rechtliche Aspekte berücksichtigt.

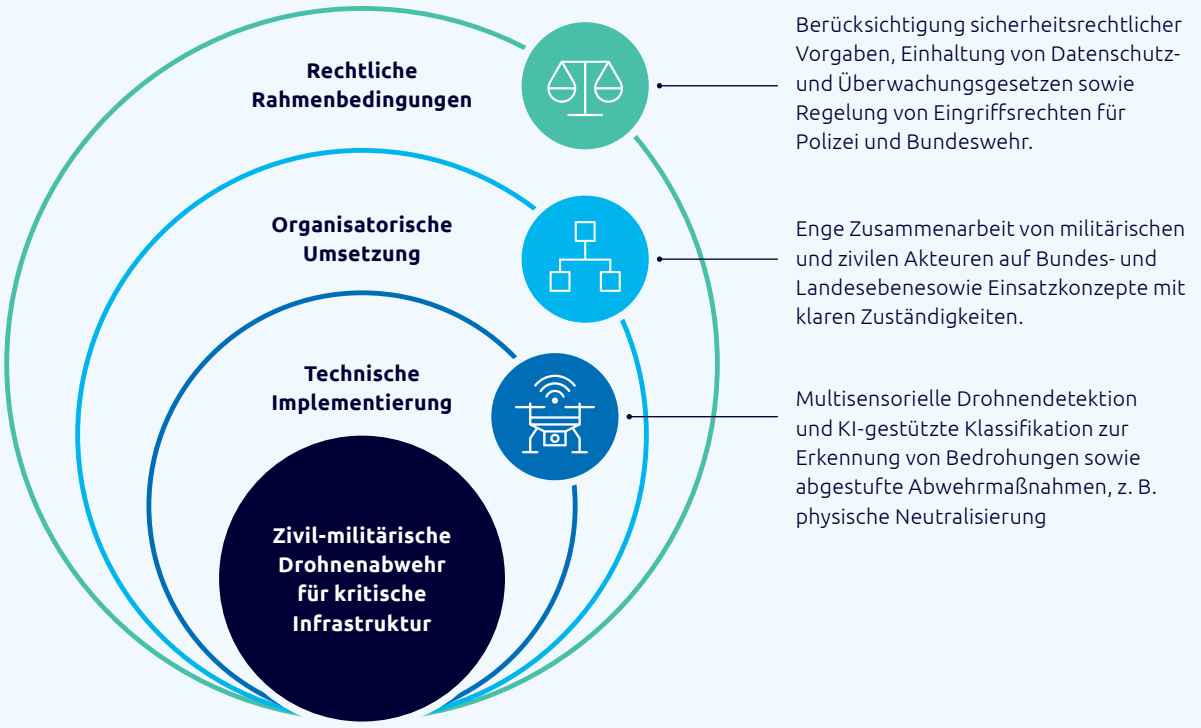
In einem **Idealszenario** nutzt ein abgestimmtes Netzwerk ziviler und militärischer Akteure multisensorielle Drohnendetektion und KI-gestützte Klassifikation, um Bedrohungen frühzeitig zu erkennen und Fehlalarme zu minimieren.

Die Abwehr erfolgt durch abgestufte Maßnahmen: von passiver Störung (Jamming, GPS-Spoofing) über physische Neutralisierung (Abfangdrohnen, Netzwerfer) bis hin zu aktiven kinetischen oder cyberbasierten Eingriffen. Die Integration in bestehende Sicherheitsnetzwerke und Frühwarnsysteme gewährleistet eine schnelle und effektive Reaktion.

Dies beginnt mit einer eng verzahnten Zusammenarbeit von Bundeswehr, Polizei, Nachrichtendiensten, KRITIS-Betreibern und internationalen Partnern. Eine gemeinsame Lagebeurteilung und Bedrohungsanalyse bildet zudem die Grundlage für ein abgestimmtes Vorgehen, während klare Zuständigkeiten und Eingriffsrechte eine rechtssichere Zusammenarbeit gewährleisten. Die Drohnenabwehr ist in die nationale Sicherheitsstrategie zu integrieren, wobei insbesondere die technologische und organisatorische Umsetzung sowie ggf. erste Landesgesetzesänderungen[28] zu berücksichtigen sind.

ABBILDUNG 6:

Konzept für zivil-militärische Drohnenabwehr



28 StMI Bayern: Schutz vor Drohnen: Ministerrat schafft klare Regeln im PAG und plant Drohnenkompetenzzentrum

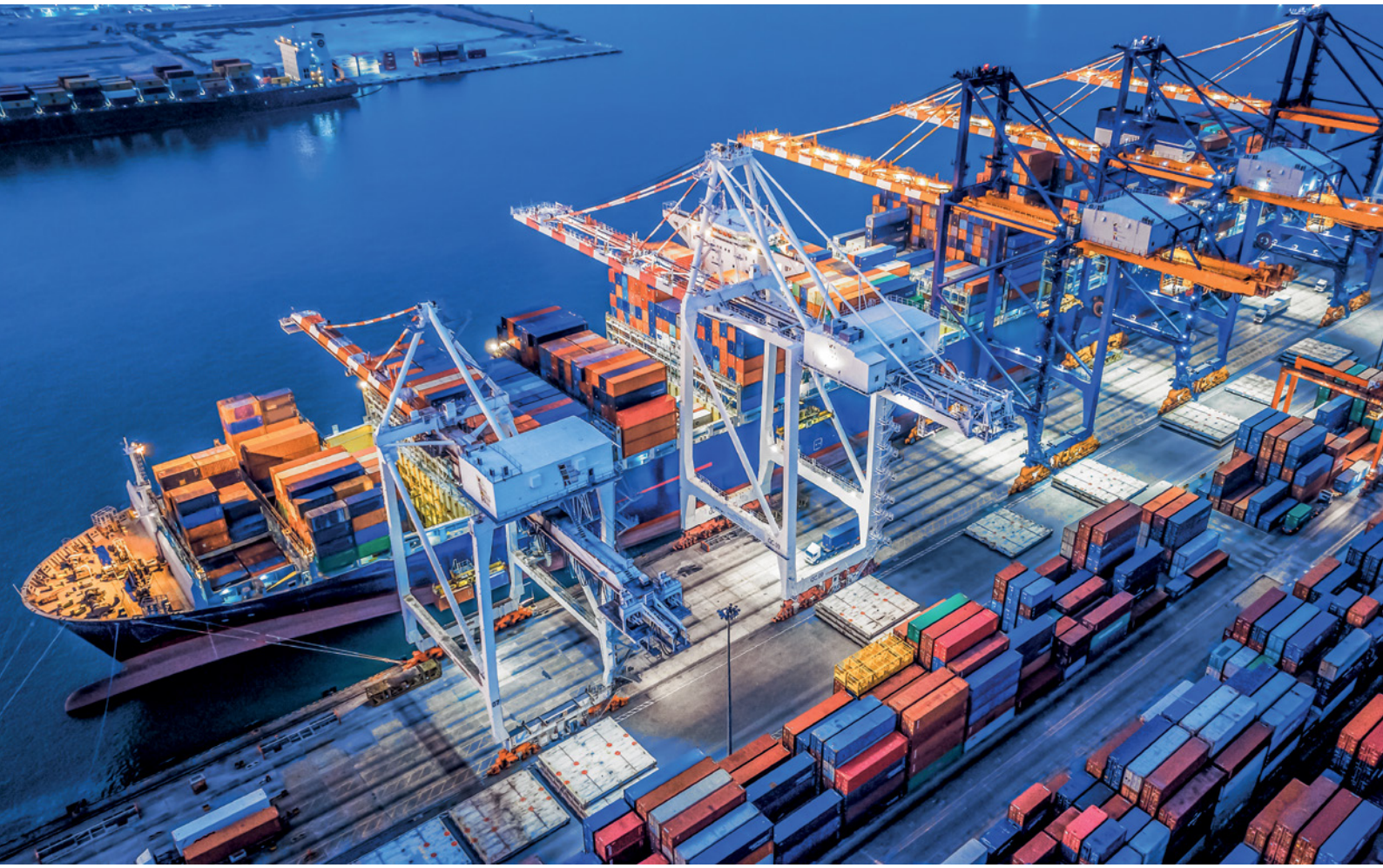
Technologische Umsetzung

Aktuelle Detektionssysteme zur Drohnenabwehr setzen auf eine Kombination verschiedener Sensortechnologien, um eine präzise Bedrohungsbewertung zu ermöglichen. Mittels Multisensordatenfusion werden Radarsysteme zur großflächigen Erfassung von Drohnenbewegungen mit optischen und Infrarotkameras kombiniert, die eine hochauflösende Identifikation und Analyse von Flugmustern ermöglichen. Ergänzend kommen akustische Sensoren zum Einsatz, die charakteristische Drohnengeräusche detektieren, sowie Hochfrequenzanalysesysteme, die Steuerungs- und Kommunikationssignale feindlicher Drohnen erfassen.

Auf Basis dieser Detektionssysteme können gezielte Abwehrmaßnahmen eingeleitet werden. Elektronische Störsysteme (Jamming) unterbrechen Navigations- und Steuersignale, während kinetische Abwehrmechanismen wie Abfangdrohnen oder Netzwerfer eine physische Neutralisierung ermöglichen. Alternativ bieten cybertechnische Eingriffe die Möglichkeit, feindliche Drohnen zu übernehmen oder auszuschalten. Ergänzend können Lasersysteme eine präzise Neutralisierung ohne Kollateralschäden ermöglichen.

Die Integration dieser Technologien in bestehende militärische und zivile Sicherheitsinfrastrukturen gewährleistet eine automatisierte Gefahrenabwehr. So entsteht ein umfassendes Schutzsystem, das flexibel auf unterschiedliche Einsatzszenarien reagieren kann und eine effektive Abwehr unautorisierter Drohnen gewährleistet.

Capgemini arbeitet eng mit entsprechenden Herstellern zusammen, die die **technischen Lösungen** zur Drohnenabwehr bereitstellen können.



Organisatorische Umsetzung

Für eine effektive Gefahrenabwehr ist eine enge Abstimmung zwischen militärischen und zivilen Akteuren erforderlich. Hierzu werden abgestimmte Krisenstäbe zwischen Bundeswehr und zivilen Behörden eingerichtet, die in gemeinsamen Lagezentren Bedrohungsanalysen durchführen und Krisensituationen bewältigen. Ergänzend werden regelmäßige Trainingsprogramme und Simulationen entwickelt, um das Sicherheitspersonal Kritischer Infrastrukturen (KRITIS) und die Streitkräfte auf reale Bedrohungsszenarien vorzubereiten.

Neben der operativen Zusammenarbeit sind klare organisatorische Rahmenbedingungen unerlässlich. Dazu gehört die eindeutige Festlegung von Zuständigkeiten, um eine effiziente Entscheidungsfindung zu ermöglichen. Dabei müssen die Befugnisse von Bundeswehr, Polizei und Betreibern kritischer Infrastrukturen klar voneinander abgegrenzt werden. Darüber hinaus sind Eskalationsstufen zu definieren, um im Verteidigungs- oder Krisenfall schnell und zielgerichtet reagieren zu können.

Ein weiterer zentraler Aspekt ist das Notfallmanagement. Standardisierte Meldeketten und Notfallpläne für Drohnenvorfälle gewährleisten eine strukturierte und schnelle Reaktion im Ernstfall. Durch diese Maßnahmen entsteht ein umfassendes Sicherheitskonzept, das eine koordinierte, abgestimmte und somit effiziente Bewältigung von Bedrohungslagen ermöglicht.

Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen für den Einsatz und die Abwehr von Drohnen basieren auf verschiedenen nationalen und internationalen Regelwerken. Auf nationaler Ebene regeln das Luftverkehrsgesetz (LuftVG) und die Luftverkehrs-Ordnung (LuftVO) den Betrieb von Drohnen, wobei unautorisierte Flüge über kritischen Infrastrukturen ausdrücklich verboten sind. Darüber hinaus gibt es Sonderregelungen, die Polizei und Bundeswehr den gezielten Einsatz von Abwehrsystemen ermöglichen. Das Grundgesetz (Artikel 35 und 87a) bildet die Grundlage für die Amtshilfe der Bundeswehr bei besonderen Gefahrenlagen, wobei eine klare Trennung zwischen polizeilichen und militärischen Befugnissen im Inland zu beachten ist. Zur adäquaten Entgegenwirkung ist eine Änderung des Luftsicherheitsgesetzes durch das Kabinett eingebracht worden.[29] Neben diesen sicherheitsrechtlichen Vorgaben spielen Datenschutz- und Überwachungsgesetze eine zentrale Rolle. Die Speicherung von Drohnendaten ist nur im Rahmen der Gefahrenabwehr zulässig und der Einsatz von Aufklärungssystemen muss den Vorgaben der Datenschutz-Grundverordnung (DSGVO) entsprechen. Damit wird sichergestellt, dass Maßnahmen zur Drohnenabwehr im Einklang mit den geltenden Datenschutzrichtlinien stehen. Auf internationaler Ebene ist die grenzüberschreitende Zusammenarbeit mit Bündnispartnern, insbesondere im Rahmen der NATO, unerlässlich. Dabei geht es sowohl um die gemeinsame Bekämpfung von Drohnenbedrohungen als auch um die Standardisierung von Abwehrmaßnahmen, um ein einheitliches und effektives Vorgehen gegen unerlaubte Drohnenaktivitäten zu gewährleisten.

Das Konzept zur zivil-militärischen Drohnenabwehr bietet einen **ganzheitlichen Ansatz**, der technologische, organisatorische und rechtliche Komponenten verknüpft. Die enge Kooperation zwischen zivilen und militärischen Akteuren sowie die Integration in bestehende Sicherheitsstrukturen sorgen für eine gesteigerte Resilienz.

29 BMI: Mehr Befugnisse für die Drohnenabwehr und den Schutz von Flughäfen

3. Militärische Mobilität und Infrastruktur

Herausforderung: Statische Mobilitätsplanung

Die Planung und Koordination von Transportvorgängen sind im Verteidigungsfall, neben der bestehenden Infrastruktur, auch stark von der Rolle Deutschlands als logistische Drehscheibe der NATO geprägt. Um dauerhaft wehrfähig zu sein, ist dabei neben militärischen Bedürfnissen auch die Aufrechterhaltung des zivilen Lebens zu berücksichtigen. Deutschland benötigt daher, mehr noch als andere Länder, einen umfassenden Blick auf das Echtzeit-Verkehrsgeschehen in der Luft, an Land und zu Wasser. Routenplanungen erfolgen dabei heute entweder mit isolierten Systemen, die auf statischen Karten basieren und dynamische Daten weitgehend unberücksichtigt lassen, oder mittels Verkehrsdaten von Anbietern mit Sitz außerhalb Deutschlands.

Lösung: Souveränes Verkehrslagebild für die zivil-militärische Mobilität

Um dieser Herausforderung zu begegnen, schlägt Capgemini die Schaffung eines **Systems zur Erfassung eines souveränen Verkehrslagebildes** vor, in dem der Zustand und die Auslastung von Straßen, Schienen-, Schifffahrts- und Luftverkehrswegen dargestellt wird.

Ein solches Verkehrslagebild ist ebenso relevant für die Nutzung in Friedenszeiten, für die Verlegung von Truppen und Übungen der Bundeswehr sowie jederzeit für das strategische Verkehrsmanagement, die effiziente Planung und Steuerung von Transporten und die Sicherstellung von Ankunftszeiten.

Die meisten für diesen Anwendungsfall erforderlichen Datenquellen sind entweder bereits öffentlich zugänglich oder können von unterschiedlichen Anbietern kommerziell erworben werden. Zudem stehen verschiedene GIS-Anwendungen – sowohl kommerzielle als auch nichtkommerzielle – zur Verfügung, die bereits in der Bundeswehr genutzt werden und als Grundlage für die Umsetzung dienen können. Ergänzend kann vorhandenes Kartenmaterial der Bundeswehr als Basis dienen, während Meldungen durch Bundeswehrangehörige ähnlich wie bei Crowdsourcingbasierten Verkehrsinformationssystemen erfolgen können. Eine mögliche Erweiterung stellt eine Routenplaner-App speziell für Bundeswehrangehörige dar.

Die Bundeswehr kann dabei weitgehend auf in der Truppe bereits heute bewährte und etablierte Technologien zurückgreifen, um das System effizient und sicher bereitzustellen. Durch den Einsatz webbasierter Lösungen kann der Zugriff über einen Browser erfolgen, während eine Android-App die Nutzung auf gesicherten Mobilgeräten ermöglicht.

ABBILDUNG 7:

Souveränes Verkehrslagebild für die militärische Mobilität

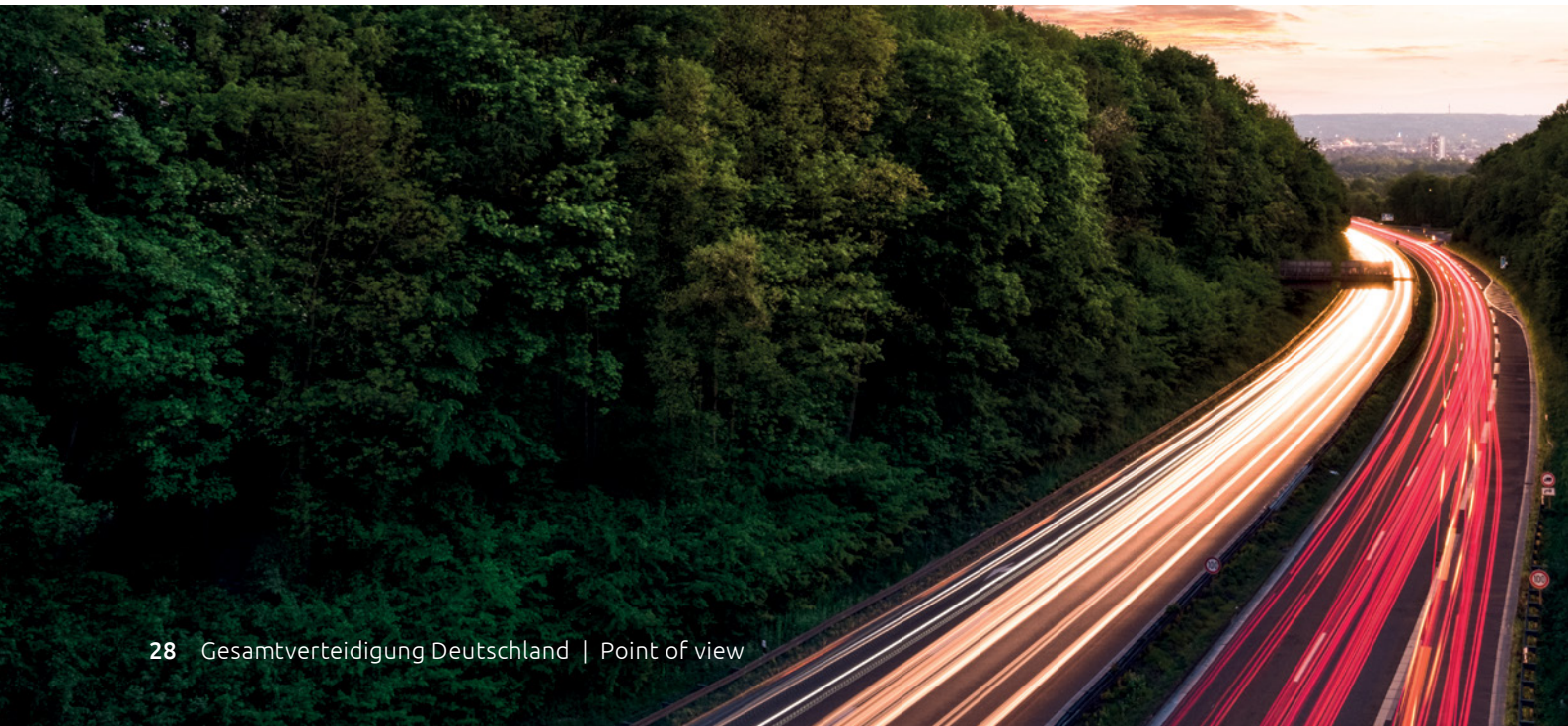
Echtzeit-Verkehrsdaten

Im Fokus des souveränen Verkehrslagebildes stehen die aktuellen Mobilitätsdaten verschiedenster Verkehrsmittel. Daten hierzu sollen es ermöglichen, optimale Routen für militärische Verlegung oder zivile Transporte zu ermitteln. Im Bereich des Straßenverkehrs stellen etwa Automobilclubs oder Verkehrsservices der Bundesländer öffentlich Echtzeitdaten zum Verkehrsaufkommen und der Verkehrsdichte bereit. Zudem werden von diesen Stellen auch Unfall- und Sperrungsmeldungen verarbeitet und aufbereitet. Mit Floating Car Data, die von Automobilherstellern kommerziell angeboten werden, können diese Echtzeitdaten erweitert werden. Der staatliche Zugriff auf diese Daten ist auch durch das VerkLG[30] gedeckt. Über öffentliche Datenplattformen wie z. B. die Mobilithek des Bundesministeriums für Verkehr werden verschiedenste Mobilitätsdaten bereitgestellt. Für die Kraftstoffversorgung von Straßenverkehrsmitteln können die Standorte von Tankstellen über die von der Markttransparenzstelle für Kraftstoffe des Bundeskartellamts zugelassenen Verbraucherinformationsdienste abgerufen werden (vgl. Anwendungsfall 1). Der Verkehr auf der Schiene kann ebenso unter Verwendung von öffentlichen Daten dargestellt werden. Das Infrastrukturregister der Deutschen Bahn liefert Daten zu Bahnstrecken und weiterer Infrastruktur. Zudem stellen die Bahnbetreiber Daten zu Baustellen und Sperrungen auf ihrer Infrastruktur bereit. Über gemeinsame europäische Systeme und öffentliche Daten zu Fahrplänen können große Teile des Schienenverkehrs in Echtzeit verfolgt und dargestellt werden.

Die Wasserstraßenverhältnisse und deren Nutzungsmöglichkeiten für die Binnenschifffahrt in Deutschland werden von der Wasserstraßen- und Schifffahrtsverwaltung des Bundes (WSV) kartografiert. Zudem können über verschiedene öffentliche Webapplikationen die AIS-Daten von Schiffen zur Echtzeit-Ortung eingesehen werden. Ähnlich wie bei den Echtzeit-Schifffahrtsdaten erfassen Stellen wie die Deutsche Flugsicherung (DFS) und weitere Applikationen die Flugbewegungen im deutschen Luftraum und darüber hinaus. Zusätzlich zu den Echtzeitdaten verschiedener Verkehrsmittel können auch Daten zu Bewegungs- und Verkehrsströmen im öffentlichen Raum auf Basis anonymisierter Signalisierungsdaten aus Mobilfunknetzen analysiert werden. Diese werden kommerziell von verschiedenen Telekommunikationsfirmen vertrieben und können ohne Verletzung der datenschutzrechtlichen Vorschriften an die Behörden übermittelt werden.

Echtzeit-Verkehrsdaten sind für ein souveränes Verkehrslagebild essenziell, da sie eine präzise und dynamische Steuerung von Transportbewegungen ermöglichen. Sie erlauben es, Verkehrsflüsse in Echtzeit zu überwachen, Engpässe frühzeitig zu erkennen und alternative Routen für militärische sowie zivile Transporte zu identifizieren, wodurch die operative Planbarkeit und Reaktionsfähigkeit erheblich verbessert wird.

30 §§ 3 I Nr. 3, 4 a.E.: „Berücksichtigt wurde aber auch die Technisierung und Digitalisierung, indem Betreiber von Informations- und Kommunikationssystemen als Verkehrsunternehmen iSd VerkLG eingestuft wurden“



Eignung und Sicherheit von Transportwegen

Militärische Fahrzeuge und Transportwege unterliegen besonderen Anforderungen, da sie häufig schwerer, größer und damit anfälliger für infrastrukturelle Einschränkungen sind als zivile Fahrzeuge. Zudem müssen sie in Krisensituationen schnell und sicher verlegt werden, was eine präzise Planung und die kontinuierliche Überwachung der Streckeneignung erfordern.

Um die Eignung von Transportwegen für militärische Konvois einzuschätzen, können Daten der Bundesanstalt für Straßen- und Verkehrswesen zur Tragfähigkeit von Brücken und Straßen genutzt werden. Gegebenenfalls kann zudem auf Daten von GST.Autobahn, einem Tool der Autobahn GmbH zur Beurteilung der Streckeneignung für Schwertransporte, zugegriffen werden.

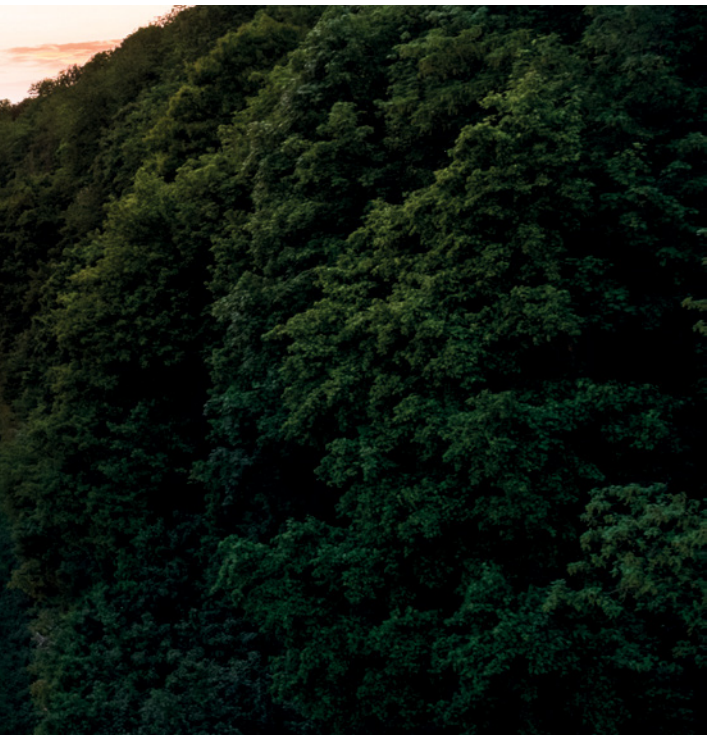
Um die Sicherheit der Transportwege weiter überprüfen zu können, kann ggf. auf die Bilder von öffentlichen Verkehrsüberwachungskameras und Mautstationen zugegriffen werden. Diese sind zwar aktuell nicht durch die Öffentlichkeit einsehbar, eine Einsicht durch Bundesbehörden ist jedoch im Krisenfall durch Berufung auf das Bundesdatenschutzgesetz (BDSG) gerechtfertigt.[31]

Auch können hier Initiativen wie der Military Routing Planner der BWI als Datenbasis aufgegriffen werden. Zur Vervollständigung eines Verkehrslagebildes ist es zudem unerlässlich, Wetter- und Witterungsbedingungen zu erfassen.

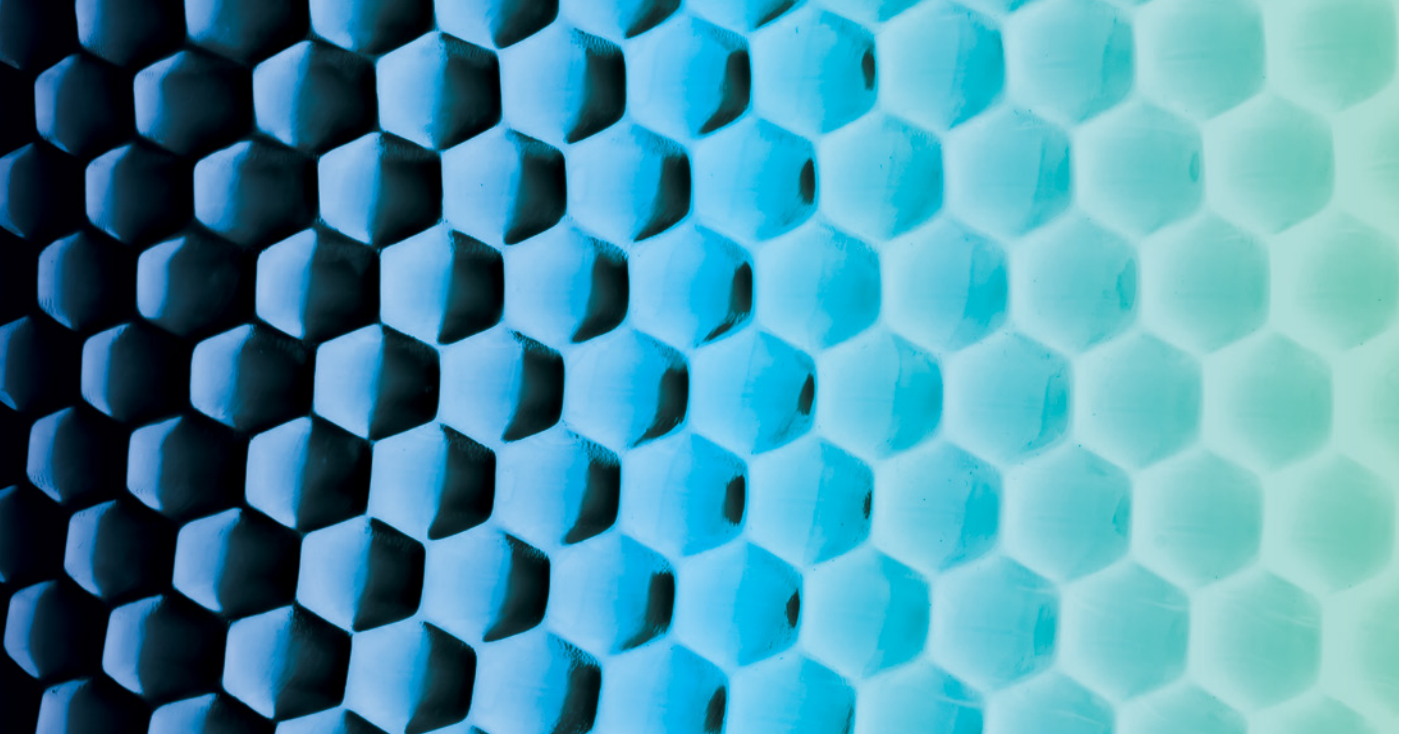
Hier können Daten des Deutschen Wetterdienstes (DWD) genutzt werden. Das ZGeoBw arbeitet in diesem Bereich bereits mit dem DWD zusammen. Durch die kombinierte Nutzung dieser Datenquellen sowie des Fachwissens vom Zentrum für Geoinformationswesen der Bundeswehr (ZGeoBw) können militärische Konvois und zivile Transporte optimal geplant werden. Geeignete Routen lassen sich identifizieren, Risiken minimieren und alternative Wege frühzeitig berücksichtigen. Ein souveränes Verkehrslagebild ist daher ein entscheidender Faktor für den Operationsplan Deutschland und die zivil-militärische Koordination. Durch die Auswertung relevanter Verkehrsdaten können Hindernisse, Engpässe und Sicherheitsrisiken frühzeitig erkannt und flexibel darauf reagiert werden, um sowohl die Einsatzfähigkeit der Streitkräfte als auch den zivilen Verkehrsfluss sicherzustellen.

Die Nutzung sicherer, national verfügbarer Datenquellen reduziert Abhängigkeiten von ausländischen Anbietern und schützt vor Manipulation und Cyberangriffen. Dies schafft bereits in Friedenszeiten einen erheblichen Mehrwert, indem es die strategische Planung von Transportkapazitäten verbessert und Synergien zwischen militärischen und zivilen Akteuren fördert. Ein souveränes Verkehrslagebild stärkt die Wehrfähigkeit, erhöht die Reaktionsgeschwindigkeit in Notlagen und leistet einen wichtigen Beitrag zur nationalen Sicherheitsarchitektur.

31 § 22 I Nr. 1 lit. c, Nr. 2 lit. c BDSG



Das souveräne Verkehrslagebild stärkt die operative Reaktionsfähigkeit der Bundeswehr, indem es militärische und zivile Mobilitätsdaten integriert, Engpässe frühzeitig sichtbar macht und die strategische Planung von Verlegungen auf Straße, Schiene, Wasser und in der Luft absichert. Damit wird die Grundlage für eine resilientere, koordinierte und zukunftsfähige militärische Mobilitätsinfrastruktur gelegt – im Krisenfall wie im Alltag.



4. Koordination und Kommunikation

Herausforderung: Gesellschaftliche Resilienz

Die aktuelle sicherheitspolitische Situation erfordert, u. a. mit Blick auf die verschärfte Bedrohungslage an der NATO-Ostflanke, eine gezielte und präventive Kommunikationsstrategie, um das Krisenbewusstsein der deutschen Bevölkerung zu stärken. Trotz wachsender militärischer Bedrohungen, externer Einflussnahme durch autokratische Staaten und hybrider Kriegsführung ist das Bewusstsein für Krisenvorsorge und gesamtgesellschaftliche Verteidigung in Deutschland bislang unzureichend ausgeprägt. Soziale Medien wie X und TikTok verstärken Polarisierung, während das Vertrauen in etablierte Medien wie den öffentlich-rechtlichen Rundfunk und Informationen, die durch staatliche Webseiten verbreitet werden, sinkt. Zudem stellen Deepfakes und KI-generierte Inhalte eine wachsende Gefahr dar, indem sie gezielt Falschinformationen über Entscheidungsträger verbreiten.[32]

In der aktuell dynamischen Sicherheitslage entscheidet nicht allein militärische Stärke, sondern auch, wie **bewusst, vorbereitet und widerstandsfähig** die deutsche Bevölkerung agiert.

32 Nature human behavior: A systematic review of worldwide causal and correlational evidence on digital media and democracy

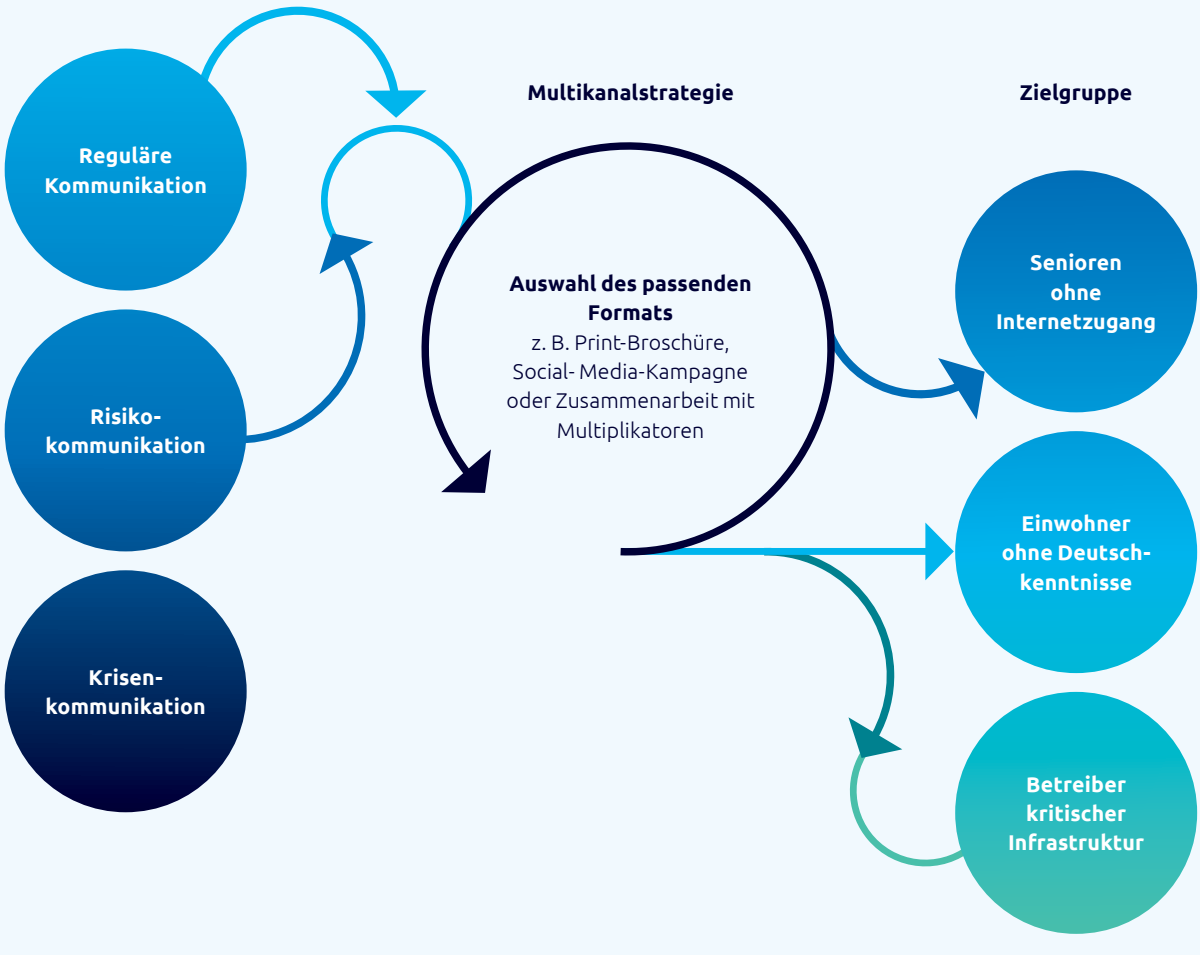
Lösung: Entwicklung einer Kommunikations-strategie zur Gesamtverteidigung

Capgemini empfiehlt die Entwicklung einer differenzierten Kommunikationsstrategie zur Gesamtverteidigung, die in reguläre, Risiko- und Krisenkommunikation unterscheidet – wie im „Leitfaden für Krisenkommunikation" des BMI vorgegeben – und auf einer Multikanal-Ansprache basiert. Das Bewusstsein für persönliche Krisenvorsorge bei militärischen Bedrohungslagen muss gesteigert und das Vertrauen in die nationale Verteidigungsfähigkeit erhöht werden. Zudem müssen Bürger grundlegendes Wissen über Schutzmaßnahmen wie Bevorratung besitzen.

Die **Steigerung der Medienkompetenz** der Bevölkerung ist ebenfalls essenziell, um der Verbreitung von Desinformation effektiv entgegenzuwirken.

ABBILDUNG 8:

Kommunikationsstrategie Gesamtverteidigung



Zielgruppen und Kernbotschaften zur gesamtstaatlichen Verteidigung

Zielgruppen werden basierend auf einer ausführlichen Stakeholder-Analyse und ähnlicher Informationsbedürfnisse gebildet. Eine Kommunikationsstrategie, die die Gesamtverteidigung Deutschlands im Blick hat, richtet sich an verschiedene Zielgruppen: Fokus dieses Anwendungsfalls sind die deutschen Staatsbürger sowie Einwohner Deutschlands ohne deutsche Staatsbürgerschaft. Daneben sollten jedoch gesellschaftliche Schlüsselakteure (z. B. Kirchen, Wohlfahrtsorganisationen wie Malteser und Johanniter und Bildungseinrichtungen wie Universitäten und Schulen), Sicherheits- und Rettungskräfte (z. B. Polizei,THW), der Gesundheitssektor, Betreiber kritischer Infrastrukturen (z. B. Energieversorgungsunternehmen wie RWE) sowie potenziell internationale Partner (z. B. NATO-Mitgliedstaaten) angesprochen werden. Zielgerichtete Kernbotschaften unterstützen die prägnante Ansprache der Zielgruppen und gewährleisten eine einheitliche Kampagnengestaltung. Die Kernbotschaften orientieren sich an drei Kommunikationsdimensionen: In der regulären Kommunikation steht der Zusammenhang zwischen gesellschaftlicher Resilienz und staatlicher Stabilität im Fokus. Die Risikokommunikation soll das Bewusstsein für persönliche Vorsorge und die Bedeutung verlässlicher Informationen stärken. In Krisenzeiten liegt der Schwerpunkt auf Gemeinschaftssinn, Besonnenheit und klarer Informationsweitergabe über offizielle Kanäle.

BEISPIELE

Zielgruppe	Reguläre Kommunikation	Risikokommunikation	Krisenkommunikation
Bevölkerung Deutschlands	„Ein stabiler Staat braucht eine resiliente Gesellschaft – jeder kann zur Sicherheit beitragen.“	„Vorsorge ist Verantwortung – rechtzeitige Vorbereitung stärkt unsere Widerstandsfähigkeit.“	„Gemeinschaft und Zusammenhalt sind unser stärkster Schutz. Wir verteidigen Deutschland gemeinsam.“

Maßnahmen und Kanäle zur Verbreitung der Botschaften

Zur Umsetzung dieser Strategie werden verschiedene Kommunikationsmaßnahmen genutzt. Reguläre Informationskampagnen über Podcasts, Social Media, Websites der Bundesministerien sowie Print- und Online-Materialien sollen ein verteidigungspolitisches Bewusstsein fördern. Die Risikokommunikation umfasst Warn-Apps, Checklisten zur Notfallvorsorge und verstärkte Aufklärung über Desinformation in sozialen Medien. In Krisensituationen wird eine schnelle, einheitliche Informationsweitergabe über TV, Radio, Warn-Apps und offizielle Regierungsseiten sichergestellt. Notfallpläne, Schutzmaßnahmen und Verhaltenshinweise werden über Anzeigesysteme an öffentlichen Plätzen und Social-Media-Kanäle verbreitet.

„97 Prozent aller Befragten wurden beim bundesweiten Warntag 2025 erfolgreich gewarnt, allein 75 Prozent über Cell Broadcast.“[33]

33 BBK: Umfrage Bundesweiter Warntag 2025: 97 Prozent der Befragten erhalten Warnung

BEISPIELE

Form	Maßnahmen	Kanäle
Reguläre Kommunikation	Aufklärung und Bildung zu verteidigungspolitischen Themen wie Bedrohungslage, Desinformation, Cybersicherheit Informationen zur Notfallvorsorge im Rahmen LV/BV wie z. B. Bevorratung, Dokumentensicherung und Notgepäck, vgl. bestehende Materialien wie „Vorsorgen für Krisen & Katastrophen" des BBK	• Bundeswehr-Podcasts (z. B. „Nachgefragt" oder „Funkkreis") • Foto-/Textbeiträge und Videos über Social Media (X, Instagram, YouTube, LinkedIn) des BMVg, Bw, BBK • Flyer und Broschüren des BBK, gedruckt und digital • Verbreitung per Post an jeden Haushalt und auf offiziellen Webseiten • Bürgerdialoge, organisiert durch BMVg, Bw und BBK
Risiko-kommunikation	Information über militärische Bedrohungslagen und Verhaltenshinweise	• Warnhinweise über Pop-up-Nachrichten und Echtzeit-Kartenmaterial über NINA-WarnApp des BBK
Krisen-kommunikation	Bundesweite Notfallkommunikation im Rahmen der LV/BV durch Sprecher der Bundesregierung	• Pressemitteilungen und Videobotschaften über Webseite der Bundesregierung • Verbreitung über öffentlich-rechtlichen Rundfunk

Verantwortlichkeiten für gesamtstaatliche Verteidigungskommunikation

Für die Umsetzung und Steuerung der Kommunikation sind verschiedene Akteure auf den föderalen Ebenen verantwortlich: Das Gemeinsame Melde- und Lagezentrum von Bund und Ländern (GMLZ) koordiniert sicherheitsrelevante Informationen bundesweit. Das BBK übernimmt die bundesweite Kommunikation zu Warnungen und Schutzmaßnahmen. Die Innenministerkonferenz ist beschlussfähig zu Kommunikationsmaßnahmen bzgl. der inneren und äußeren Sicherheit auf Landesebene.

Öffentlich-rechtliche Medien wie ARD (inkl. ihrer Landesrundfunkanstalten) und ZDF greifen in Krisen offizielle Informationenund Warnmeldungen von Behörden und Regierung auf und berichten darüber, um die Bevölkerung zu informieren. Krisenstäbe auf Kreisebene bzw. in Stadtverwaltungen tragen Verantwortung auf kommunaler Ebene. Zudem tragen Social-Media-Teams der Ministerien und Fact-Checking-Initiativen aktiv zur Bekämpfung von Desinformation bei.

Die gesamtstaatliche Verteidigung erfordert eine **gezielte Kommunikationsstrategie**, die das Krisenbewusstsein stärkt, Desinformation entgegenwirkt und die Widerstandsfähigkeit der deutschen Bevölkerung erhöht. Dafür sichert eine differenzierte, multikanalbasierte Ansprache effektive Aufklärung, fördert gesellschaftliche Resilienz und gewährleistet klare Informationsweitergabe in Krisenzeiten.

Was unsere *Experten* sagen

Marc Akkermann
Vice President
Head of Public Defense Germany
Capgemini

„Eine gesamtstaatliche Verteidigungsfähigkeit und Resilienz ist in der heutigen Zeit das übergeordnete Ziel der Ausrichtung der Bundeswehr, und das unter Einbeziehung diverser anderer Ressorts. Der Operationsplan Deutschland ist eine wesentliche Initiative in diesem Umfeld. Die Weiterentwicklung der zivil-militärischen Zusammenarbeit, datenbasiert, interoperabel und unter Beachtung der Anforderungen an Informationssicherheit und Datenschutz, ist in diesem Kontext essenziell. Eine solcher Angang erfordert einen souveränen Datenraum für das Ressourcenmanagement und die Koordination in der Gesamtverteidigung. Dazu zählen Handlungsfelder wie die Integration resilienter, cloudbasierter Infrastrukturen und digital gestützter Kollaborationslösungen. Der Einsatz datengestützter Technologien, klare Governance-Strukturen sowie technologieoffene, skalierbare Architekturen gelten als zentrale Erfolgsfaktoren für eine widerstandsfähige Sicherheitsstruktur. Unsere Erfahrungswerte aus über zwei Jahrzehnten an der Schnittstelle von öffentlicher Sicherheit, IT und Behördenkommunikation fließen in diese Entwicklungsperspektive mit ein."

Thilo Zelt
Executive Vice President
Head of Public Sector Germany
Capgemini Invent

„Die aktuelle Sicherheitslage zeigt deutlich: Gesamtstaatliche effektive Verteidigung braucht keine zusätzliche Bürokratie, sondern strategische Klarheit und handlungsfähige Strukturen. Verteidigung ist dabei auch eine Frage leistungsfähiger eigenverantwortlicher Organisationen. Verwaltungen sollten nicht auf andere warten, sondern mit smarter IT-Governance, engagierten Fachkräften und wirksamen Prozessen aktiv Verantwortung übernehmen. Das Vertrauen der Bürgerinnen und Bürger in Staat und Wirtschaft wird sich künftig auch daran messen, wie entschlossen die Sicherheitsinfrastruktur modernisiert wird."

Carmen-Valentina Ciocoi
Senior Director
Head of Public Defense Germany
Capgemini Invent

„In sicherheitskritischen Zeiten ist es entscheidend, gesellschaftliche Widerstandsfähigkeit nicht nur technologisch, sondern auch organisatorisch, kommunikativ und kulturell zu stärken. Nachhaltige Veränderung gelingt insbesondere durch lernende Organisationen und partnerschaftliche Umsetzung. Darüber hinaus ist das Ziel, durch strategische Kommunikation Vertrauen zu schaffen, die Öffentlichkeit einzubinden und Krisenkompetenz zu stärken. Damit können Bürgerinnen und Bürger als aktive Mitgestaltende von Sicherheit gewonnen werden – durch verständliche Informationen, partizipative Formate und einen Stil, der nicht belehrt, sondern befähigt."

Dr. Mark Dornbach
Director
Data Driven Public
Capgemini Invent

„Die Fähigkeit, Daten intelligent zu strukturieren und strategisch nutzbar zu machen, ist ein zentraler Hebel für Resilienz und Steuerungsfähigkeit im Kontext der Gesamtverteidigung. Dazu gehören der Aufbau leistungsfähiger Datenplattformen, die nahtlose Vernetzung verteilter Systeme sowie die Entwicklung tragfähiger Datenstrategien, insbesondere in hochregulierten Umfeldern wie dem Verteidigungsbereich. Die Herausforderung liegt nicht nur in der technischen Umsetzung, sondern in der Schaffung übergreifender und interoperabler Ökosysteme, die unterschiedlichen Akteuren einen gesicherten regelbasierten Zugang zu relevanten Informationen ermöglichen. Beratung in diesem Umfeld heißt daher, technologischen Tiefgang mit einem strukturierten Blick auf Governance, Skalierbarkeit und Zukunftsfähigkeit zu verbinden."

Adresse
Capgemini Deutschland GmbH
Potsdamer Platz 5
10785 Berlin

Autorinnen und Autoren
Carmen-Valentina Ciocoi, Marc Akkermann, Dr. Mark Dornbach, Juri Denecke

Publikationsjahr
2026

Über Capgemini
Capgemini ist ein globaler Partner für die KI-gestützte Geschäfts- sowie Technologietransformation. Das Unternehmen schafft messbaren Mehrwert für seine Kunden, indem es die Zukunft von Organisationen gestaltet und im Zusammenspiel von KI, Technologie sowie dem Mensch Realität werden lässt. Seit fast 60 Jahren steht Capgemini für Verantwortung wie auch Vielfalt und beschäftigt 420.000 Mitarbeitende in über 50 Ländern. Das End-to-End-Leistungsspektrum gründet auf einer umfangreichen Branchenexpertise, einem starken Partner-Ökosystem sowie Kompetenzen in den Bereichen Strategie, Technologie, Design, Engineering und Operations. Die Gruppe erzielte 2024 einen weltweiten Umsatz von 22,1 Milliarden Euro.

Make it real | www.capgemini.com/de