Sandra Bubendorfer-Licht MdB
Leon Eckert MdB
Dr. André Hahn MdB
Dr. Günter Krings MdB
Ingo Schäfer MdB

GRÜNBUCH ZMZ 4.0

Zivil-Militärische Zusammenarbeit 4.0 im militärischen Krisenfall

Eine Situationsbeschreibung, Analyse und Handlungsempfehlungen

INHALT

VORWORT

Die **Zivil-Militärische Zusammenarbeit (ZMZ) in Deutschland hat durch die verstärkte sicherheitspolitische Bedrohung durch Russland** – insbesondere seit der Annexion der Krim 2014 und dem russischen Angriffskrieg gegen die Ukraine 2022 – an Bedeutung gewonnen. Die sicherheitspolitische Strategie einer Pazifizierung Russlands durch enge wirtschaftliche Verflechtungen hat sich als Fehler erwiesen. Die aktuelle geopolitische Lage zwingt Deutschland und seine Partner dazu, die Resilienz ihrer Gesellschaft und Infrastruktur gegen militärische, nicht-militärische und hybride Bedrohungen zu stärken. Dabei nimmt die Zusammenarbeit zwischen zivilen Akteuren und der Bundeswehr eine zentrale Rolle ein.

Die ZMZ soll im Rahmen der neuen sicherheitspolitischen Realität erweitert werden, da der Schwerpunkt seit dem Kalten Krieg auf Katastrophenhilfe und Amtshilfe lag. Die veränderte Bedrohungslage erfordert nun eine stärkere Ausrichtung auf die Resilienz gegenüber hybriden Bedrohungen und die Ausrichtung auf die Landes- und Bündnisverteidigung.

Dieses GRÜNBUCH zeigt dringende Handlungserfordernisse auf, beschränkt sich dabei auf ausgewählte Bereiche und konzentriert sich auf den Bereich der Vorbereitung von Landes- und Bündnisverteidigung (ZMZ **4.0**). Ziel ist es, ausgehend von Szenarien, erste wichtige Aspekte dieser großen gesamtstaatlichen Aufgabe der ZMZ zu beleuchten.

Die inhaltlich-thematische Logik der numerischen Ordnung „Zivil-Militärische-Zusammenarbeit 4.0“ (einfließend in die Begrifflichkeit „GRÜNBUCH „ZMZ **4.0**“) leitet sich historisch wie folgt ab:

ZMZ 1.0: Zivil-Militärische Zusammenarbeit unter den Annahmen und Bedingungen der bipolaren Konfrontation mit Betrachtung Kriegsschauplatz Deutschland bis 1989/90.

ZMZ 2.0: Zivil-Militärische Zusammenarbeit als Civil Military Cooperation (CIMIC) in den Auslandseinsätzen der Bundeswehr als Bestandteil einer militärischen und zivilen Gesamtstrategie zur Unterstützung der Auftragserfüllung.

ZMZ 3.0: Zivil-Militärische Zusammenarbeit in der Amts- und Katastrophenhilfe neuer nationaler Krisendimensionen (Flüchtlingshilfe; Corona; Hilfe bei Flut und Hochwasser und Waldbrandereignissen).

ZMZ 4.0: Zivil-Militärische Zusammenarbeit in der Re-Fokussierung auf Landes- und Bündnisverteidigung und als Instrument der Gesamtverteidigung, auch unter den Bedingungen asymmetrischer und hybrider Konflikte unterhalb des Spannungs- und Verteidigungsfalls (Operationsplan Deutschland – OPLAN DEU).

ZUSAMMENFASSUNG FÜR POLITIK, VERWALTUNG UND WIRTSCHAFT

Die hybride Kriegsführung Russlands und die Einflussnahme anderer Staaten auf Deutschland erfordern ein Umdenken in der Sicherheits- und Außenpolitik. Bevölkerung, politische Entscheidungsträger und Verwaltung müssen koordiniert und entschlossen reagieren. Das erfordert, Schwächen zu adressieren, die Resilienz auf allen Ebenen zu stärken und die Prinzipien einer regelbasierten internationalen Ordnung zu verteidigen. Nur so kann verhindert werden, dass autoritäre Akteure wie Russland ihre Strategien erfolgreich weiterführen.

Die Gesamtverteidigung hat mit den wachsenden sicherheitspolitischen Herausforderungen erheblich an Bedeutung gewonnen. Sie muss gewährleisten, dass Deutschland auf ein breites Spektrum von Bedrohungen vorbereitet ist – von militärischen Konflikten über Cyberangriffe bis hin zu Naturkatastrophen. Sie bleibt ein wesentlicher Bestandteil der Sicherheitsstrategie Deutschlands und erfordert eine enge Zusammenarbeit zwischen Staat, Gesellschaft, Wirtschaft und internationalen Partnern.

Die **Zivil-Militärische Zusammenarbeit** (ZMZ) ist ein Bestandteil der Zivilen Verteidigung und trägt damit zur Gesamtverteidigung bei. Sie beschreibt unter anderem das **Zusammenwirken von staatlichen oder nichtstaatlichen zivilen Organisationen mit den Streitkräften im Bereich der Bündnis- und Landesverteidigung.**

Im militärischen Krisenfall liegt der Schwerpunkt der ZMZ in der Unterstützung der Streitkräfte (vgl. Abb. 1).

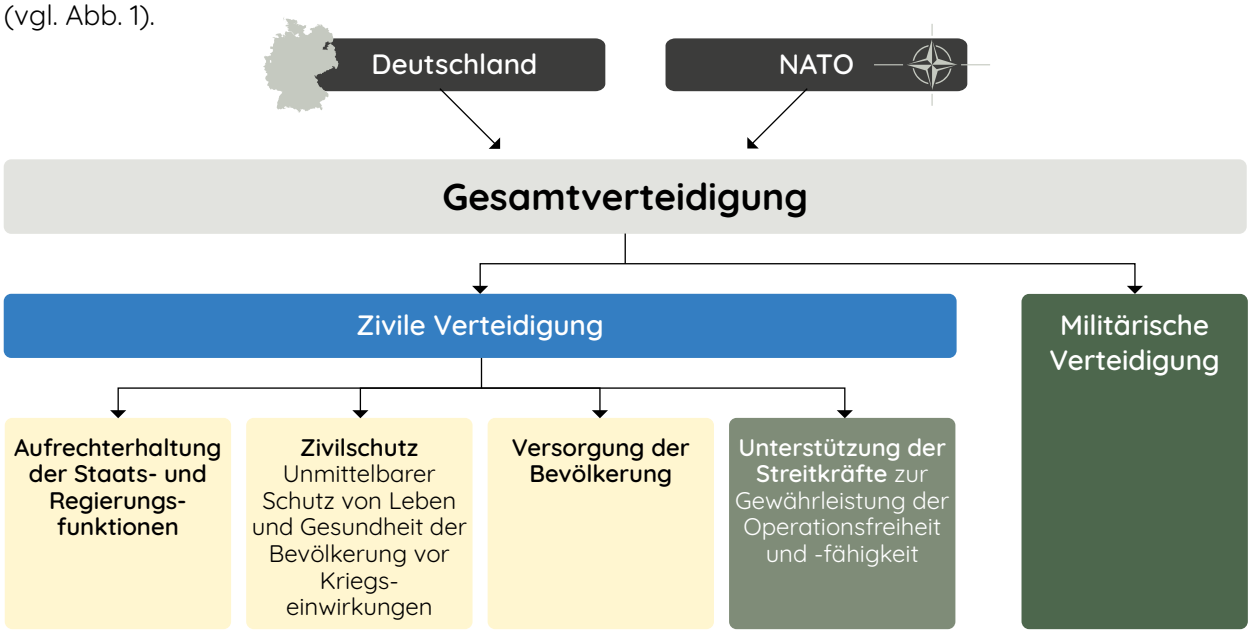

Abbildung 1: ZMZ als Teil der Gesamtverteidigung

Russlands hybride Kriegsführung, die sich über mehr als ein Jahrzehnt erstreckt, und die neue militärische Bedrohung stellen eine grundlegende Herausforderung für westliche Staaten und deren Sicherheitsstrukturen dar. Die Konsequenzen, die daraus zu ziehen sind, umfassen in Deutschland mehrere Bereiche:

Abschreckung zur Friedenssicherung
Eine glaubwürdige Abschreckung funktioniert nur, wenn Deutschland auch über die hinreichenden Fähigkeiten verfügt, insbesondere die Bundeswehr im militärischen Krisenfall unterstützen zu können. Hierfür müssen der Zivilschutz als ein Element der Zivilen Verteidigung entsprechend ertüchtigt und Investitionsstaus aufgelöst werden.

Gesamtgesellschaftliche Verantwortung
Die ZMZ basiert auf dem Prinzip der gegenseitigen Unterstützung und erfordert ein hohes Maß an Kooperation und Vertrauen. Gleichzeitig ist sie ein Ausdruck gesamtgesellschaftlicher Verantwortung, da sie zeigt, dass Sicherheit und Resilienz nur im Zusammenspiel aller Akteure gewährleistet werden können.

Gesellschaftlicher Zusammenhalt
Die Integration militärischer Unterstützung in zivile Prozesse bedarf einer ehrlichen Kommunikation der Bedrohungslage, muss transparent, demokratisch legitimiert und stets am Gemeinwohl orientiert sein. Dies fördert Vertrauen in staatliche Strukturen und Maßnahmen.

Im Hinblick auf ZMZ bedarf es daher einer breiten gesellschaftlichen Sensibilisierung, damit Bürgerinnen und Bürger und Institutionen ihre jeweilige Rolle kennen und im Notfall handlungsfähig bleiben. Zum gesellschaftlichen Zusammenhalt zählt auch die Einbindung und Integration unterschiedlicher Bevölkerungsgruppen in die staatlichen Institutionen der Gefahrenabwehr.

Stärkung der Resilienz
Die moderne Gesellschaft ist stark von funktionierenden Infrastrukturen (Energie, Wasser, Informationstechnologie, Kommunikation, Transport) abhängig. Dies gilt auch für den Bereich der Unterstützung der Streitkräfte. Angriffe auf diese Systeme können im militärischen Krisenfall dramatische Auswirkungen haben. Deshalb sind Entscheidungen in Politik und Verwaltung auch unter Berücksichtigung militärischer Gesichtspunkte zu treffen. Der Staat muss entsprechende Vorgaben für die Verwaltung und Wirtschaft machen, um Kritische Infrastrukturen effektiv zu schützen.

Organisation und Strukturen
Die ZMZ im militärischen Krisenfall erfordert eine feste organisatorische Verankerung auf Bundes-, Landes- und kommunaler Ebene, die mit klarer Verantwortungszuweisung verbunden ist. Im Krisenfall muss klar sein, wer welche Aufgaben übernimmt.

Insgesamt werden im GRÜNBUCH zahlreiche Handlungsnotwendigkeiten aufgezeigt und konkrete Handlungsempfehlungen formuliert, die dazu beitragen sollen, die Zivil-Militärische-Zusammenarbeit vor dem Hintergrund der veränderten Bedrohungslage zukunftsorientiert weiterzuentwickeln. Hierfür sind grundsätzliche (politische) Entscheidungen erforderlich. Im Interesse der Sicherheit Deutschlands sind insofern auch auskömmliche Haushaltsmittel auf allen Ebenen bereitzustellen.

Wirksame ZMZ 4.0 ist handlungsleitend für Entscheidungsträgerinnen und Entscheidungsträger in Politik, Verwaltung und Wirtschaft, um mögliche Aggressoren abzuschrecken, die Bundesrepublik Deutschland verteidigen zu können und die freiheitlich demokratische Grundordnung zu schützen.

HERAUSGEBERIN UND HERAUSGEBER

Sandra Bubendorfer-Licht MdB
Leon Eckert MdB
Dr. André Hahn MdB
Dr. Günter Krings MdB
Ingo Schäfer MdB

MITWIRKENDE

Kernteam

Leitung

Wolfgang Lohmann, Vorstand ZOES e. V., Inspekteur BPdL im BMI a. D.

Christian Seel, Gesamtvorstand ZOES e. V., Staatssekretär a. D. und Beauftragter für Zivil-Militärische Zusammenarbeit und Bevölkerungsschutz im Ministerium für Inneres, Bauen und Sport des Saarlandes

Mitarbeitende

Oberst i. G. Thorsten Alme
Bundeswehr/Territoriales Führungskommando (TerrFüKdo)

Oberst i. G. Armin Schaus
Bundeswehr/TerrFüKdo

KptLt Tobias Bothner
Bundeswehr/TerrFüKdo

Oberst Martin Ruske
Bundeswehr/Landeskommando Brandenburg

Dr. Dr. Dirk Freudenberg
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Vizepräsident Sinan Selen
Bundesamt für Verfassungsschutz

Frank Weber
Malteser Hilfsdienst e. V.

Dr. Berthold Stoppelkamp
Bundesverband der Sicherheitswirtschaft

Dr. Jürgen W. O. Harrer
Universität der Bundeswehr München

Dr. Wolfgang Zink
PricewaterhouseCoopers WPG GmbH

Klaus Göz
PricewaterhouseCoopers WPG GmbH

Marcus Schulze
PricewaterhouseCoopers WPG GmbH

Daniel Ehlers
PricewaterhouseCoopers WPG GmbH

Torsten Voß
Landesamt für Verfassungsschutz Hamburg

Anja Domres
Landesamt für Verfassungsschutz Hamburg

Berthold Witting
Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern

Uwe Becker
Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern

Hartfrid Wolff
Bundesministerium für Digitales und Verkehr

Das vorliegende GRÜNBUCH „ZMZ 4.0“ wurde vom Kernteam erstellt. Es basiert auf umfassenden, fachlichen Recherchen und der Einbindung zahlreicher Expertinnen und Experten, unter anderem in einem Workshop „Zukunftsforum spezial“ für Mitglieder des ZOES. Die Ausführungen spiegeln nicht notwendigerweise die politischen Positionen der Herausgeberschaft in Gänze wider.

Teilnehmende am „Zukunftsforum spezial“ – Kompetenzplattform ZMZ

Leitung

Christian Seel, Gesamtvorstand ZOES e. V., Staatssekretär a. D. und Beauftragter für Zivil-Militärische Zusammenarbeit und Bevölkerungsschutz im Ministerium für Inneres, Bauen und Sport des Saarlandes

Kerstin Alps-Rydberg
Stromnetz Berlin GmbH

Robin Bangard
Büro Sandra Bubendorfer-Licht MdB

Günther Batschak
Deutsches Rotes Kreuz e. V.

Markus Bensmann
Malteser Hilfsdienst e. V.

Mathias Beßel
Deutscher Feuerwehrverband

Andreas Bläse
Deutsche Lebens-Rettungs-Gesellschaft e. V.

Albrecht Broemme
Vorstandsvorsitzender Zukunftsforum Öffentliche Sicherheit e. V.

Sandra Bubendorfer-Licht
Mitglied des Deutschen Bundestages

Désirée Bychara-Hahn
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Anja Domres
Landesamt für Verfassungsschutz Hamburg

Frank Drescher
Malteser Hilfsdienst e. V.

Andreas Effinger
SAS Institute GmbH

Daniel Ehlers
PricewaterhouseCoopers WPG GmbH

Annegret Ernst
Johanniter-Unfall-Hilfe e. V.

Prof. Dr. Frank Fiedrich
Bergische Universität Wuppertal

Cécile Fradet-Kraft
Bundeswehr/Territoriales Führungskommando (TerrFüKdo)

Benno Fritzen
Deutsches Institut für Normung e. V.

Prof. Dr. Clemens Gause
Verband für Sicherheitstechnik e. V.

Dr. Thomas Gawlowski
Bundesministerium für Bildung und Forschung

Otto Gies
Airbus Defence and Space GmbH

Anna Gossing
Bundesakademie für Sicherheitspolitik

Andrej Gross
Deutsche Messe AG

Robert Hanz
R+V Allgemeine Versicherung AG

Michaela Haseneder
Deloitte GmbH

Oliver Hauner
Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Björn Hawlitschka
MACONIA GmbH

Andre Hermann
Deloitte GmbH

Robin Herweg
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Vizepräsident Hans-Hermann Höltje
Deutsche Lebens-Rettungs-Gesellschaft e. V.

MinDirig Dr. Christoph Hübner
Bundesministerium des Innern und für Heimat

Laura Jeske
e*Message W.I.S. Deutschland GmbH

Gerd-Jürgen Jooß
Fujitsu Germany GmbH

Dominik Kampmann
Moody´s Analytics Deutschland GmbH

Julian Karwath
Bundesamt für Strahlenschutz

Uwe Kirsche
Deutscher Wetterdienst

Dr. Katharina Kloke
Bundesministerium für Bildung und Forschung

Holger Könnecke
MACONIA GmbH

Mareike Kortmann
Esri Deutschland GmbH

Dr. Simone Kraatz
Technisches Hilfswerk

Saruna Kudevita
Bundesamt für Verfassungsschutz

Stephanie Lehmann
BEN Berlin Energie- und Netzholding GmbH

Martin Lesti
Bundeswehr/Territoriales Führungskommando (TerrFüKdo)

Guido Linge
Dräger Safety AG & Co. KGaA

Wolfgang Lohmann
Vorstand ZOES e. V.

Daniel Lücking
Büro Dr. André Hahn MdB

Nils Lüttschwager
Büro Leon Eckert MdB

Dirk Nopens
e*Message W.I.S. Deutschland GmbH

Dr. Celia Norf
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Prof. Dr. Harald Olschok
Hochschule für Wirtschaft und Recht Berlin

Dr. Eri Park

Ivo Pestel
R+V Allgemeine Versicherung AG

Dr. Sigurd Peters
Deutsch-Europäische Kommission für Bevölkerungsschutz e. V.

Kai Pietsch
Technisches Hilfswerk

Jonas Rarbach
Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e. V.

Oberst Andreas Reitz
Bundeswehr/Territoriales Führungskommando (TerrFüKdo)

Dr. Klaus Ritgen
Deutscher Landkreistag

Oliver-Patrick Rodewald
Johanniter-Unfall-Hilfe e. V.

Dr. Jens Römer
Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Miriam Rühr
50Hertz Transmission GmbH

Daniel Schaetzler
Kompetenzzentrum Kritische Infrastrukturen e. V.

Ulf-Michael Schildt
Esri Deutschland GmbH

Stefan Schröter
Airbus Defence and Space GmbH

Dr. Naomi Shulman
Forschungsforum Öffentliche Sicherheit

Prof. Dr. Ingo J. Timm
Universität Trier/Deutsches Forschungszentrum für Künstliche Intelligenz

Stefan Truthän
CATONKA Investment GmbH

Sven O. Weirup
European Aviation Security Center e. V.

1 Ausgangsüberlegung/Einleitung

Mit dem russischen Angriff auf die Ukraine am 24. Februar 2024 haben sich die Anforderungen an die deutsche Sicherheits- und Verteidigungspolitik fundamental geändert. Zum ersten Mal seit Jahrzehnten muss wieder von einer militärischen Bedrohung ausgegangen werden.

Bundesverteidigungsminister Boris Pistorius macht deutlich:

> *„Der Krieg ist mit Putins brutalem Angriff gegen die Ukraine nach Europa zurückgekehrt. Damit hat sich die Bedrohungslage verändert. Deutschland muss als bevölkerungsreichstes und wirtschaftlich starkes Land in der Mitte Europas das Rückgrat der Abschreckung und kollektiven Verteidigung in Europa sein."*

Krieg wird erneut als Mittel der Politik genutzt, um Grenzen zu verschieben und das Prinzip der Macht des Stärkeren zu etablieren. Dem muss eine verteidigungsfähige Gesellschaft und Politik entgegenstehen, die auf die Prinzipien des Völkerrechts setzt und bereit ist, sich auch gegen hybride Angriffe zur Wehr zu setzen.

Das Thema Zivil-Militärische Zusammenarbeit (ZMZ) ist vor diesem Hintergrund heute wichtiger denn je und muss grundlegend definiert werden. ZMZ 4.0 geht über die Amtshilfe nach Art. 35 Grundgesetz (GG) hinaus.

Indes ist es von zentraler Bedeutung, dort die **Wurzeln der aktuellen Diskussion** zu identifizieren. Wie kam es zu dem Wiederaufleben der Frage, unter welchen Voraussetzungen Streitkräfte im Innern eingesetzt werden dürfen? Zeitlich rückte die Bundeswehr bei der Bewältigung der **Flüchtlingskrise** 2015 erstmalig flächendeckend in den Fokus der Länder und des Bundes. Der Betrieb der Software zur Registrierung der Flüchtlinge wäre ohne die Bundeswehr nicht durchhaltefähig möglich gewesen. Das System der Erfassung und Verteilung wäre seinerzeit folglich zusammengebrochen. Abgesehen von weiteren zahlreichen „klassischen" Amtshilfeverfahren wie der Unterstützung beim Aufbau von Zelten oder dem Verbringen von Personen in die Kommunen zeigt, welches Potenzial in der ZMZ bei der Verzahnung der Streitkräfte und ziviler Akteure in der Bewältigung von Lagen steckt.

Augenfällig wurde dieses notwendige Potenzial weiterhin durch die vielen helfenden Hände bei der Bekämpfung von **Waldbränden** oder **Hochwasserkatastrophen**, wobei jeweils ein gehöriger Anteil durch technische Hilfe noch hinzukommt.

Ein weiteres positives Beispiel war der Einsatz der Streitkräfte in der **Corona-Pandemie**. Von der Unterstützung in Testzentren über die Kontaktnachverfolgung, die Testungen in Heimen bis hin zur Unterstützung bei den Impfzentren war die Bundeswehr mit ihren Möglichkeiten unverzichtbarer Teil der Lösung der jeweiligen Probleme.

Der Einsatz der Bundeswehr bei der **Amts- und Katastrophenhilfe** nach Art. 35 GG ist ein wichtiger Bestandteil staatlicher Krisenbewältigung geworden. Sie ist in der öffentlichen Wahrnehmung nicht mehr wegzudenken und damit in der Mitte der Gesellschaft angekommen. Dadurch hat die Bundeswehr auch einen deutlichen Imagegewinn in der öffentlichen Wahrnehmung erzielt. An dieser Stelle ist aber auch festzuhalten, dass diese Aufgaben nicht zu den Kernaufgaben der Streitkräfte gehören. Mit der häufigen Bindung der Bundeswehr in der Amts- und Katastrophenhilfe und der politischen Entscheidungen zur Finanzierung zahlt sie und damit unser Staat einen Preis in Form der Vernachlässigung ihrer ursprünglichen eigentlichen Aufgaben, der Landes- und Bündnisverteidigung (LV/BV). Die zunehmenden

Aufgaben im Rahmen der **Landes- und Bündnisverteidigung erfordern den konsequenten Ausbau der Kapazitäten der anerkannten Hilfsorganisationen, um Amts- und Katastrophenhilfe nur noch in Ausnahmefällen aus Kapazitäten der Streitkräfte zu gewährleisten** – nach der Fokussierung auf Auslandseinsätze seit den 1990er Jahren, wie zum Beispiel auf dem Balkan, in Afghanistan und in Afrika. Auch dort wurde in einem deutlichen Maß auf die ZMZ gesetzt, um Aufgaben vor Ort zu erfüllen. International als Civil Military Cooperation (CIMIC) bezeichnet, ist die Verbindung zu zivilen Autoritäten anderer Staaten und die Unterstützung beim Aufbau ziviler Strukturen das Ziel.

Der Bedarf an Zivilschutz wird durch den **Ukraine-Krieg** wieder in das Bewusstsein der Bevölkerung gerückt. Die Hoffnung auf einen lange währenden Frieden in Europa sind 2014 bereits ins Wanken geraten und spätestens mit dem russischen Agieren im Februar 2022 erloschen.

Die aktuelle Diskussion sollte daher über die Schnittstelle von Bundeswehr und zivilen Strukturen hinausgehen.

LV/BV soll absehbar nicht nur geübt, sondern auch praktiziert werden. Das Verteidigungsministerium ist gefordert, einen Beitrag unterhalb der Schwelle in einem **NATO-Bündnisfall** zu leisten. Anders als im Kalten Krieg der 1970er und 1980er Jahre ist Deutschland kein Frontstaat mehr, sondern wird seine Rolle als **Drehscheibe** finden und beweisen müssen. Mensch und Material werden in großem Umfang durch Deutschland verbracht und auf dem Weg hier versorgt werden. Wir müssen uns zum Beispiel darauf einstellen, dass Verwundete hier klinisch folgeversorgt werden müssen, inklusive der Rehabilitation, bis sie wieder zum Einsatz entlassen werden.

Wie sind die beiden Bereiche Amtshilfe und LV/BV zu betrachten? Kurz gesagt, die Hilfeleistungen fließen in unterschiedliche, sogar gegensätzliche Richtungen. Während bei der Amtshilfe die Streitkräfte die Länder und die Gebietskörperschaften unterstützen, ist es bei LV/BV andersherum. In dem zu erwarteten Szenario ist Deutschland nicht mehr Frontstaat und wird als Drehscheibe zum Transitland. Eigene und alliierte Truppen verlegen an die Ostflanke der NATO, was ohne die Unterstützung der Länder und der kommunalen Familie nicht leistbar ist. Amtshilfe und LV/BV verhalten sich also wie **zwei Seiten derselben Medaille**, die Sicherheit in Deutschland heißt. Beide Bereiche sind ohne eine Verschränkung am Ende nicht denkbar, weil sich alle Ebenen der staatlichen Gewalt gegenseitig unterstützen müssen, um die innere und äußere Sicherheit erfolgreich zu gewährleisten.

Die innere Sicherheit schließt im weiteren Sinne auch die **Resilienz im Bevölkerungsschutz** ein. Hier ist die Brücke in die wichtigen Bereiche auch außerhalb der Streitkräfte im Rahmen der ZMZ zu schlagen. Eine wirksame ZMZ 4.0 kann nur gelingen, wenn die zivilen Strukturen, angefangen auf der Bundesebene, ihre Verantwortlichkeit erkennen. Resilienz hat viel mit dem Schutz vitaler Fähigkeiten und Infrastrukturen wie zum Beispiel Sicherheit, Verkehr, Energie, Krankenversorgung zu tun und ist eine gesamtstaatliche Aufgabe, die nicht allein dem Bundesministerium der Verteidigung obliegt. Der Operationsplan Deutschland (OPLAN DEU) ist eine wichtige Säule und der Anfang einer Planung, die auf alle Bereiche staatlichen Handelns ausgedehnt werden muss.

Die **vertikale und horizontale Vernetzung** der staatlichen Ebenen (Kommunen, Gebietskörperschaften, Länder und der Bund) muss in alle Richtungen, auch innerhalb der jeweiligen Ebene, optimiert werden. Die zivilen Akteure sind ebenso einzubeziehen wie Nichtregierungsorganisationen (NGO).

Mit diesem **GRÜNBUCH** soll ein **erster Impuls** gegeben werden, wie unter anderem diese Vernetzung gelingen kann.

Besondere Bedeutung erlangen im Zusammenhang mit ZMZ 4.0 resiliente Kritische Infrastrukturen (KRITIS).

In einer zunehmend vernetzten und komplexen Welt sind der Schutz und die Aufrechterhaltung Kritischer Infrastrukturen für das reibungslose Funktionieren unserer Gesellschaft von essenzieller Bedeutung. KRITIS wie Energieversorgung, Wasserwirtschaft, Informationstechnologie und Transport sind das Rückgrat moderner Staaten. Ihre Störung oder Zerstörung kann weitreichende Folgen haben, die das öffentliche Leben, die Wirtschaft und die Sicherheit gefährden.

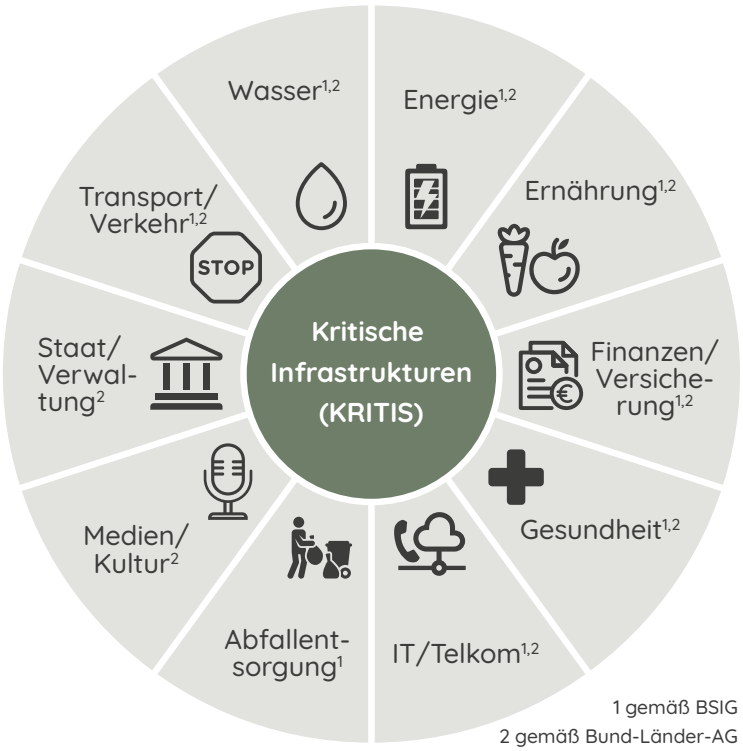

Abbildung 2: Kritische Infrastrukturen

Verteidigungswichtige Kritische Infrastruktur (VKI) bezeichnet jene Infrastruktureinrichtungen und -systeme, die für die nationale Sicherheit und Verteidigungsfähigkeit eines Staates von besonderer Bedeutung sind. Ihre Funktionsfähigkeit muss in Krisenzeiten oder bei Bedrohungen aufrechterhalten werden, da sie die Grundlage für die Abwehr von Bedrohungen, die Aufrechterhaltung der staatlichen Ordnung und die Fähigkeit zur Selbstverteidigung bilden.

In diesem Zusammenhang spielt die ZMZ eine zentrale Rolle. Gerade in zivilen oder militärischen Krisenfällen erweist sich die enge Abstimmung und Kooperation zwischen zivilen Behörden und militärischen Kräften als entscheidend, um schnell und effizient auf Bedrohungen zu reagieren und die Versorgungssicherheit zu gewährleisten.

Dieses GRÜNBUCH beleuchtet die Bedeutung von ZMZ im Kontext des Schutzes von KRITIS, aufbauend auf dem beschriebenen Grundszenario Mai 2030 mit fiktiven, aber realistischen weiterführenden KRITIS-Szenarien.

Auf Grundlage eines Ausgangsszenarios werden die Herausforderungen analysiert und erforderliche Maßnahmen zur effektiven Zusammenarbeit im militärischen Krisenfall, im Schwerpunkt aber auf zivile Unterstützung der Streitkräfte im Krieg oder mögliche Eskalationsschwellen im Frieden – ZMZ 4.0 beschrieben.

2 Situationsbeschreibung, veränderte Ausgangslage für ZMZ

Die aktuelle Bedrohungslage zeigt, die Friedensdividende ist nun endgültig aufgebraucht. Wir befinden uns zwar noch nicht im Krieg, aber wir befinden uns auch schon lange nicht mehr im Frieden. Wir befinden uns in einer Phase dazwischen, einer sogenannten Grauzone, charakterisiert durch einen Nebel hybrider Taktiken. In modernen Kriegsszenarien setzen Angreifer zunehmend auf eine Kombination aus klassischen Militäreinsätzen und hybriden Taktiken, so genannter hybrider Kriegsführung. Dabei geht es im Kern um Einflussnahme, unter anderem durch militärische, propagandistische, wirtschaftliche und kulturelle Mittel. Ziel ist es, die öffentlichen Meinungen zu beeinflussen, eine Gesellschaft und Staatsform zu destabilisieren. Offene pluralistische und demokratische Gesellschaften bieten im Vergleich zu autoritären Staaten in der Regel mehr Angriffsflächen und sind ohne Vorhaltung entsprechender Abwehrmechanismen leicht verwundbar. Besonders und zugleich herausfordernd ist die Verschleierungstaktik. Die Täter operieren entweder anonym oder bestreiten Beteiligungen an Vorfällen und Konflikten. Intensität und Attribution sind somit die zwei wesentlichen Hebel und Schwellen, welche uns zudem die Verwobenheit von innerer und äußerer Sicherheit vor Augen führen.

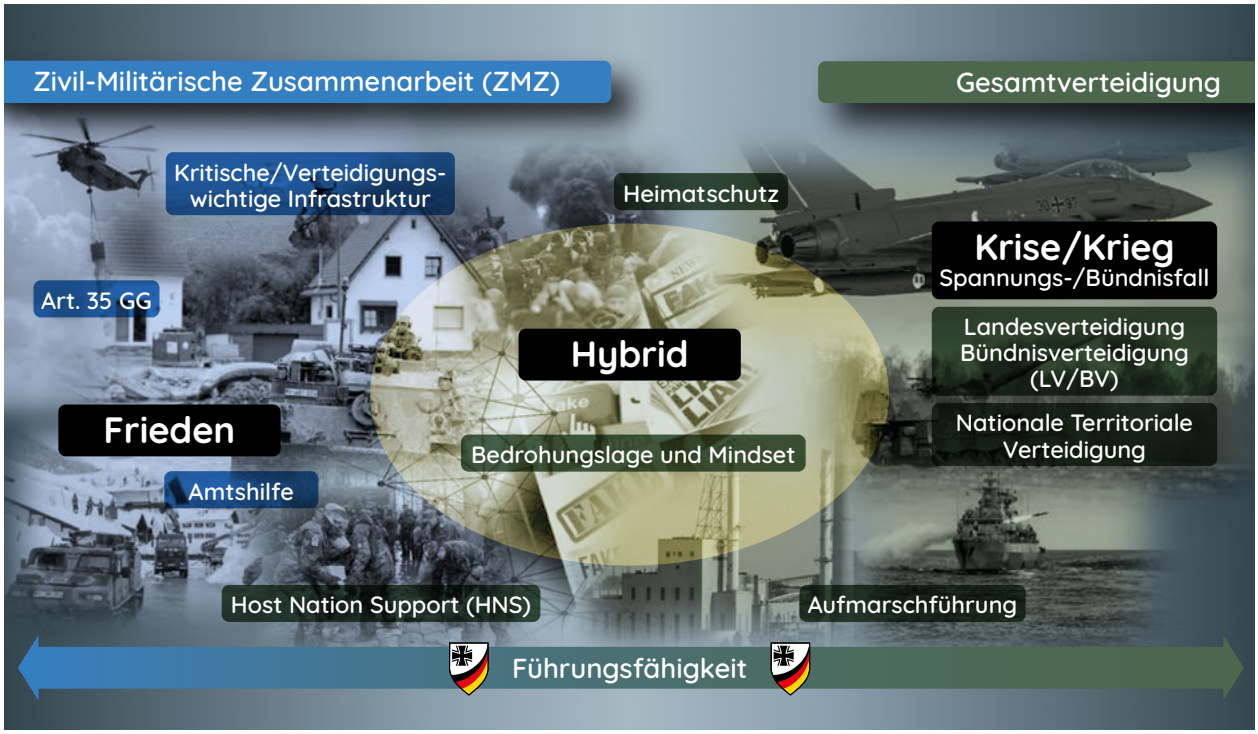

Abbildung 3: Hybride Bedrohungslage

Diese Art der Kriegsführung kann man insbesondere im russischen Krieg gegen die Ukraine beobachten. Aber auch wir sind dieser Bedrohung bereits heute und das beinahe täglich ausgesetzt, nämlich in Form von Fake News/Desinformation, Cyberangriffen sowie Ausspähung und sogar Sabotage.

Das GRÜNBUCH „Zivil-Militärische Zusammenarbeit 4.0“ beschreibt eine Weiterentwicklung des Zusammenwirkens von staatlichen und nichtstaatlichen zivilen Organisationen mit den Streitkräften im Bereich der Bündnis- und Landesverteidigung. Diese ist erforderlich aufgrund der veränderten geopolitischen Lage, die durch multiple weltweite Krisen und Kriege und nicht zuletzt in Europa durch den von Russland ausgelösten Krieg in der Ukraine entstanden ist.

Europa und auch Deutschland müssen auf diese veränderte Bedrohungslage reagieren. Deshalb ist eine Sensibilisierung der nationalen Entscheidungsträger auf Bundes-, Landes- und kommunaler Ebene unbedingt erforderlich. Das vorliegende GRÜNBUCH gibt dazu konkrete Handlungsanleitungen, die allerdings auch noch der rechtlichen und insbesondere finanziellen Unterfütterung bedürfen. Die Stärkung der Resilienz kritischer Anlagen oder der Aufbau einer modernen und durchschlagkräftigen Cyberabwehr erfordert noch viel mehr unsere Aufmerksamkeit als bisher.

Es ist Zeit, die vor uns liegenden Aufgaben anzupacken.

– Dr. Günter Krings MdB

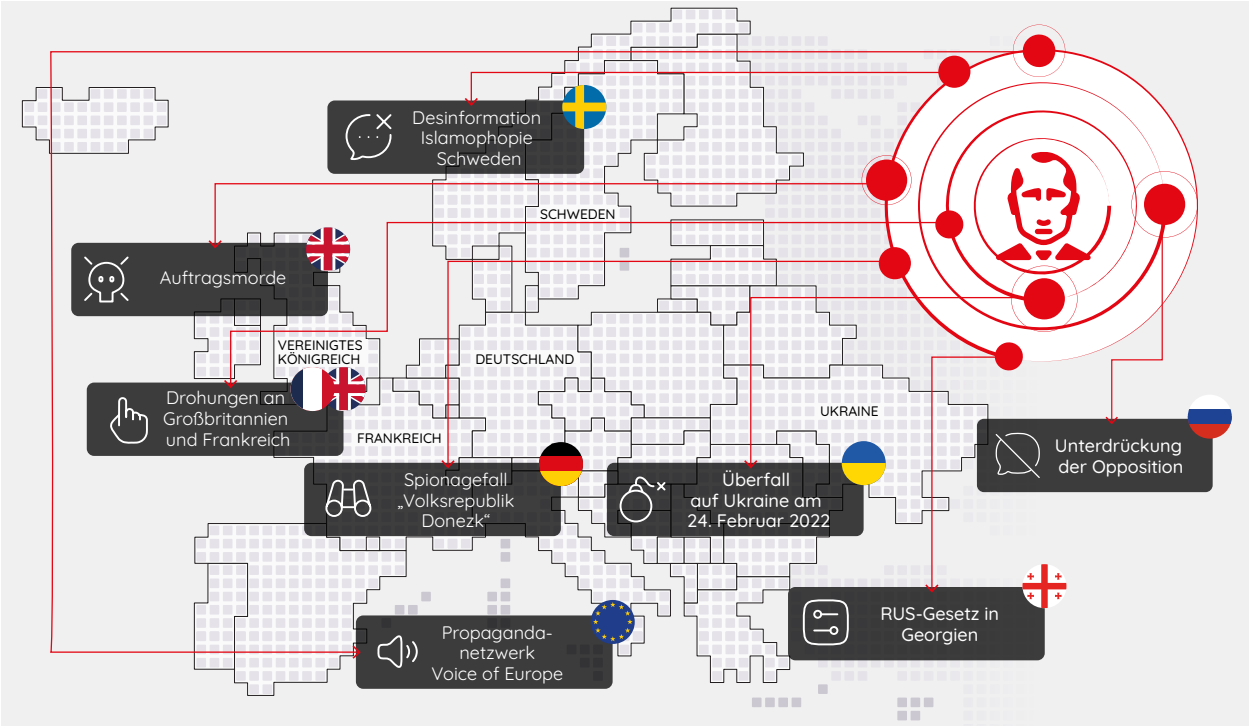

Abbildung 4: Konkrete Bedrohungen

Integrierte Sicherheit

Putins Krieg hat uns gezeigt, dass unsere Sicherheit nicht selbstverständlich ist. Als wirtschaftlich starkes Land, mit gefestigter Demokratie und starken Partnern an unserer Seite, stellen wir uns den aktuellen Herausforderungen mit Selbstvertrauen sowie Zuversicht. Die Nationale Sicherheitsstrategie (2023) soll hierfür Grundlage und Wegweiser sein. Mit einer Politik der Integrierten Sicherheit soll Deutschland wehrhaft, resilient und nachhaltig werden.

Die Sicherheit Deutschlands betrifft alle Menschen und ist nur durch das Zusammenwirken aller staatlichen Ebenen, der Wirtschaft und Gesellschaft zu erreichen. Zudem ist sie untrennbar mit der Sicherheit unserer Alliierten und europäischen Partner verbunden.

Unverzichtbares Fundament deutscher, europäischer und transatlantischer Sicherheit ist eine glaubwürdige Abschreckungs- und Verteidigungsfähigkeit. Folgerichtig ist die Landes- und Bündnisverteidigung wieder Kernauftrag deutscher Streitkräfte.

Der Ansatz Integrierter Sicherheit erfordert allerdings die gemeinsame und einheitliche Betrachtungsweise der militärischen und der zivilen Verteidigung. Aufgrund der starken Wechselwirkungen zwischen äußerer und innerer Sicherheit hängt die Handlungsfähigkeit Deutschlands nach außen zunehmend auch von seiner Resilienz im Inneren ab. Auf Bundesebene ist das Bundesministerium der Verteidigung (BMVg) neben dem Bundesministerium des Innern und für Heimat (BMI) ein Schlüsselressort für die Umsetzung einer wirksamen Gesamtverteidigungsfähigkeit Deutschlands. Es richtet derzeit die Fähigkeiten der Bundeswehr zur Landes- und Bündnisverteidigung umfassend neu aus.

Der Operationsplan Deutschland

Eine Ableitung dieser Neuausrichtung war die Aufstellung des Territorialen Führungskommandos der Bundeswehr im Jahr 2022, das im Schwerpunkt für die Planung, Führung und Koordination von Operationen der Bundeswehr innerhalb Deutschlands verantwortlich war. Für den militärischen Anteil zur nationalen Gesamtverteidigung sowie in Ableitung der NATO-Verteidigungspläne entwickelte ein Team aus Expertinnen und Experten aller Bereiche der Bundeswehr, des Bundes, der Länder und Kommunen, der sogenannten Blaulichtorganisationen und der Wirtschaft den Operationsplan Deutschland (OPLAN DEU).

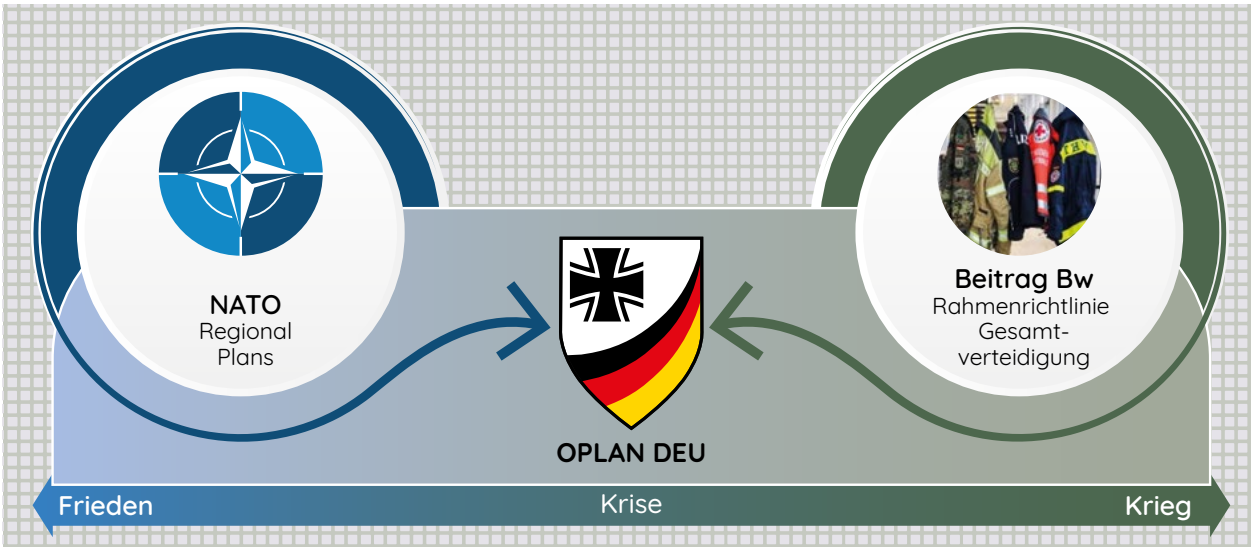

Abbildung 5: Operationsplan Deutschland (OPLAN DEU)

„Deutschland. Gemeinsam. Verteidigen.“ ist Ziel und Maßstab dieser Zusammenarbeit.

Der OPLAN DEU ist ein geheimes, hoch adaptives Dokument, das stetig weiterentwickelt wird. Es umfasst den Einsatz der Bundeswehr in Deutschland in Frieden, Krise und Krieg und damit die Bandbreite von Heimatschutz bis zur Nationalen Territorialen Verteidigung. Die wesentliche Aufgabe Deutschlands im Bündniskontext besteht darin, den geplanten Aufmarsch und die Versorgung verbündeter und eigener Streitkräfte, insbesondere durch Host Nation Support (HNS), als „Drehscheibe Deutschland“ sicherzustellen.

Sofern notwendig, muss demnach eine signifikante Anzahl von Soldatinnen und Soldaten mit ihrem Material durch Deutschland transportiert und dabei durchgängig logistisch sowie medizinisch versorgt und geschützt werden. Die dafür erforderliche Unterstützung als Transit- und Gastnation ist keine rein militärische, sondern eine gesamtstaatliche Aufgabe.

Zu diesem Zweck werden im OPLAN DEU Anforderungen an die Bundeswehr und andere staatliche sowie zivile Akteure im Rahmen der gesamtstaatlichen Verteidigung festgehalten, neben anderem die zivil-militärische Interaktion zur gegenseitigen gesamtstaatlichen Unterstützung, die Maximierung ziviler Leistungserbringung, der Schutz lebens- und verteidigungswichtiger (Infra-)Strukturen sowie der Heimatschutz bis hin zur Nationalen Territorialen Verteidigung.

Der OPLAN führt also die zentralen militärischen Anteile der Landes- und Bündnisverteidigung und der dafür erforderlichen zivilen Unterstützungsleistungen in einem Plan zusammen, der im Ergebnis ausführbar ist. Er trifft damit die planerische Vorsorge dafür, dass im Krisen-, Konflikt- und Kriegsfall nach erfolgter politischer Entscheidung schnell, zielgerichtet und im verfassungsrechtlichen Rahmen gehandelt werden kann. Zugleich soll er impulsgebend für die Entwicklung eines Plans zur Gesamtverteidigung mit dem Ziel Integrierter Sicherheit sein.

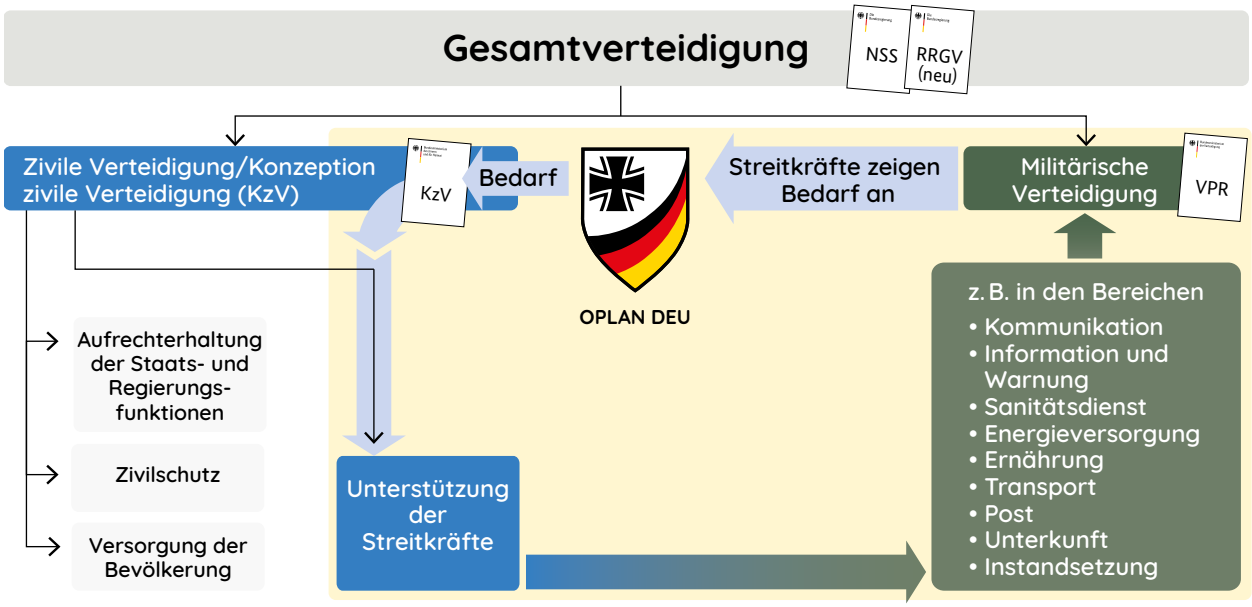

Abbildung 6: Unterstützung der Streitkräfte

Militärische und zivile Verteidigung sind und bleiben organisatorisch zwar eigenständig, stehen jedoch im Rahmen der Gesamtverteidigung in einem engen und unauflösbaren Zusammenhang. Mit der Rahmenrichtlinie Gesamtverteidigung vom 5. Juni 2024 stärkt die Bundesregierung in einem weiteren Schritt die zivile und militärische Verteidigung und sichert damit unter anderem auch die zivile und logistische Unterstützung für die Streitkräfte. Damit wurde eine wesentliche Voraussetzung für die weitere Umsetzung des OPLAN DEU geschaffen.

Bundeswehr der Zeitenwende

Neben der Erarbeitung und stetigen Weiterentwicklung des OPLAN DEU werden in der Bundeswehr weitere Maßnahmen umgesetzt.

Erstmals stationiert die Bundeswehr eigene Truppen in Stärke einer Brigade schwerer Kräfte dauerhaft beim Bündnispartner Litauen an der NATO-Ostflanke, der durch seine direkte Grenze zu Russland besonders bedroht ist. Die Bundeswehrangehörigen werden dort gebraucht und sind willkommen – so, wie einst ständig mehr als eine Millionen Angehörige alliierter Truppen bis in die 1990er Jahre jahrzehntelang die Sicherheit Deutschlands an der damaligen NATO-Ostflanke garantiert haben. Unsere Soldatinnen und Soldaten leisten dort einen sichtbaren Beitrag zur Abschreckung und Verteidigungsfähigkeit des Bündnisses. Im Jahr 2027 soll die Brigade einsatzfähig sein.

Darüber hinaus wurde mit dem „Osnabrücker Erlass“ die Grundlage für eine neue Struktur der Bundeswehr geschaffen, um diese für den Verteidigungsfall optimal aufzustellen. Unter Heranziehung des Territorialen Führungskommandos der Bundeswehr und des Einsatzführungskommandos der Bundeswehr wurde das Operative Führungskommando der Bundeswehr zum 1. Oktober 2024 aufgestellt. Es ist damit zentrale Ansprechstelle für alle operativen Belange unserer Verbündeten und multinationalen Organisationen wie NATO und EU sowie für deutsche Behörden und Organisationen mit Sicherheitsaufgaben auf Bundes- und Landesebene. Die Struktur der Landeskommandos als Ansprechpartner für die Landesregierungen in territorialen Fragen hat sich besonders bewährt. Sie bleiben als Sensoren „in der Fläche“ erhalten. Die Heimatschutzkräfte werden künftig dem Heer zugeordnet, um eine bestmögliche Vorbereitung auf den Bündnis- und Verteidigungsfall bereits im Grundbetrieb sicherzustellen. Diese Kräfte würden dann nämlich in der Dimension Land eingesetzt.

Damit sind nach vielen Jahren planerischer Zurückhaltung außerordentlich anspruchsvolle Aufgaben unter den Vorzeichen eines möglichen, von außen aufgezwungenen Krieges definiert. Diese gewinnen mit der angekündigten Notwendigkeit des Generalinspekteurs der Bundeswehr, innerhalb von fünf Jahren kriegstüchtig werden zu müssen, zusätzlich an Relevanz und unterstreichen, wie sehr unsere Verteidigung einer gesamtstaatlichen und gesamtgesellschaftlichen Anstrengung bedarf.

> *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. Denn auch die Menschen in den Unternehmen, Verwaltungen oder zivilen Einsatzorganisationen leisten im Ernstfall einen unverzichtbaren Beitrag für die Sicherheit der Menschen in Deutschland.*
>
> *Um im Ernstfall zusammenwirken zu können, müssen der zivile und militärische Bereich eng verzahnt und koordiniert werden. Die Anstrengungen der bisherigen Bundesregierung bleiben hinter diesen Erwartungen zurück. Für diese komplexe Aufgaben bietet das GRÜNBUCH einen wichtigen Impuls.*
>
> *– Leon Eckert MdB*

3 Gesamtgesellschaftliche Verantwortung

Die Zivil-Militärische Zusammenarbeit (ZMZ) ist ein zentraler Bestandteil der gesamtgesellschaftlichen Verantwortung, da sie dazu beiträgt, die Resilienz einer Gesellschaft in Krisenzeiten zu stärken. Sie ist ein integraler Bestandteil moderner Sicherheits- und Vorsorgestrukturen. Sie basiert auf dem Prinzip der gegenseitigen Unterstützung und erfordert ein hohes Maß an Kooperation und Vertrauen. Gleichzeitig ist sie ein Ausdruck gesamtgesellschaftlicher Verantwortung, da sie zeigt, dass Sicherheit und Resilienz nur im Zusammenspiel aller Akteure gewährleistet werden können.

ZMZ basiert auf der engen Kooperation zwischen zivilen Organisationen, Behörden, der Bevölkerung und den Streitkräften, um die neuen Herausforderungen effektiv zu bewältigen. Eine widerstandsfähige Gesellschaft erfordert den Schulterschluss aller Akteure – von der lokalen Bevölkerung bis hin zu staatlichen Institutionen. Die Bevölkerung selbst spielt eine wichtige Rolle, indem sie im Sinne der Zivilen Verteidigung geschult und sensibilisiert wird.

Denn erfolgreiche ZMZ wird nur dann gelingen, wenn jede und jeder Einzelne aus der Bevölkerung daran aktiv mitwirkt. Hierzu ist das kollektive Bewusstsein zu schaffen und aufzubringen. Dies setzt vonseiten politischer Verantwortungsträgerinnen und -träger zunächst einen Kommunikationsstil voraus, der sicherheitspolitische Herausforderungen klar benennt, die Grenzen der staatlichen Unterstützungsfähigkeit beschreibt und Bürgerinnen und Bürgern Wege der Eigenvorsorge an die Hand gibt. Die Realität von vielfältigen Milieus und Lebensmodellen einer modernen Einwanderungsgesellschaft sind hierbei in Ansprache und Kommunikation anzuerkennen, um Vertrauen und Partizipation zu stärken. Wo kann ich meinen Anteil leisten? Bestenfalls im ehrenamtlichen Engagement oder im beruflichen Teil des Lebens, aber sicher auch als verantwortungsvolle Bürgerin und Bürger dieses Landes. Wie kann ich meine persönliche Resilienz stärken? Dies beginnt bei der Einlagerung von Vorräten oder allgemein bei der Vorbereitung auf Mangellagen. Aber auch den solidarischen Anteil an der Sicherstellung und Aufrechterhaltung der Strukturen, die zum Überleben gebraucht werden, ist in den Blick zu nehmen. Erfolgreiche ZMZ lebt vom Mitmachen, vom Mitdenken und vom Annehmen der Umstände.

Organisationen wie das Technische Hilfswerk (THW), das Deutsche Rote Kreuz, Johanniter, Malteser oder andere NGOs arbeiten oft eng mit den Streitkräften zusammen und zeigen, wie wichtig zivilgesellschaftliches Engagement ist.

> *Zu den Kernaufgaben im Rahmen der leider notwendigen Zeitenwende gehört eine deutlich intensivere Zivil-Militärische Zusammenarbeit. Das müssen wir verinnerlichen und bei unserer politischen Arbeit konsequent nach außen tragen.*
>
> *Wirksame Bündnisverteidigung sowie pro-aktive Abschreckung gelingen nur, wenn Staat und Gesellschaft an einem Strang ziehen. Dabei sind Resilienz und Selbstbefähigung entscheidende Faktoren, wenn es darum geht, dass jede und jeder Einzelne dazu beitragen kann und will, unser Land umfassend gegen Angriffe von außen zu schützen.*
>
> *– Sandra Bubendorfer-Licht MdB*

4 Beschreibung des allgemeinen Rechtsrahmens und der NATO-Verpflichtungen

4.1 Rechtlicher Rahmen für die Erfüllung der Aufgaben in der Zivil-Militärischen Zusammenarbeit

In Deutschland ist die Zivil-Militärische Zusammenarbeit (ZMZ) ein integraler Garant für die innere und äußere Sicherheit sowie die deutsche Leistungsfähigkeit als logistische Drehscheibe der NATO im Falle eines Truppenaufmarsches. Sie ermöglicht die Bewältigung komplexer Aufgaben durch die Multiplikation vorhandener Kompetenzen sowie die bedarfsgerechte Nutzung bestehender Kapazitäten. Bereits in Friedenszeiten kommt ihr daher sicherheitspolitisch eine besondere Bedeutung zu. Die rechtlichen Rahmenbedingungen für ZMZ variieren je nach Szenario und lassen sich in drei Hauptgruppen unterscheiden.

4.1.1 Friedensfall – Katastrophenfall/ Terrorismusbekämpfung

In Deutschland wird der Katastrophenfall durch eine Vielzahl von Gesetzen und Verordnungen geregelt, die sowohl auf Bundes- als auch auf Landesebene existieren. So ermöglichen **Art. 35** und **Art. 87 a Abs. 4** in Verbindung mit **Art. 91** des **Grundgesetzes (GG)** den Einsatz der Streitkräfte im Inland für Naturkatastrophen und besonders schwere Unglücksfälle sowie den länderübergreifenden Einsatz von Polizeikräften, etwa für Terrorismusbekämpfung. Daneben regelt primär das **Zivilschutz- und Katastrophenhilfegesetz (ZSKG)** die Zusammenarbeit zwischen Bund und Ländern im Katastrophenfall. So übernimmt der Bund gemäß **§§ 1-4 ZSKG** die Verantwortung für den Zivilschutz **(ZS)**, während die Länder für den Katastrophenschutz (KatS) in Friedenszeiten zuständig sind. Diese spielen eine zentrale Rolle, da sie über eigene Katastrophenschutzbehörden verfügen und Einsatzkräfte mobilisieren können, die auf regionale Besonderheiten und Gefahrenlagen spezialisiert sind. Die Durchführung der damit einhergehenden Maßnahmen wird im Rahmen der Bundesauftragsverwaltung aus **Art. 85 GG** primär durch die Kommunen beziehungsweise Kreise als Bündelungsbehörden gesteuert. Der **§ 16 ZSKG** erlaubt es, im Katastrophenfall Ressourcen des Bundes wie das Technische Hilfswerk (THW) und die Bundespolizei zur Unterstützung der Länder heranzuziehen. **§ 12 ZSKG** verzahnt im Sinne des Doppelnutzens somit den friedenszeitlichen Katastrophenschutz und den Zivilschutz. Die **Landeskatastrophenschutzgesetze** regeln die spezifischen Aufgaben und Zuständigkeiten der lokalen Behörden. Beispielhaft ist hier das **Bayerische Katastrophenschutzgesetz (BayKSG)** anzuführen, das in **Art. 5** die Aufgaben der Katastrophenschutzbehörden definiert. Die enge Zusammenarbeit zwischen Bundes-, Landes-, Kreis- und Kommunalebene im Rahmen des Föderalismus ermöglicht es dadurch, eine vertikale Integration aller beteiligten Akteure zu gewährleisten und eine effiziente Ressourcenallokation sicherzustellen.

4.1.2 Spannungs- und Konfliktfall

Landesverteidigung

Sollte ein Verteidigungsfall gem. **Art. 115a GG** festgestellt und verkündet sein oder durch die Bundesregierung eine drohende Gefahr für den Bestand oder die freiheitliche demokratische Grundordnung des Bundes oder eines Landes gem. **Art. 87a Abs. 4, 2 HS** festgestellt werden, werden die Streitkräfte gem. **Art. 87a GG** ermächtigt, im Inland tätig zu werden. In einem solchen Fall kann die Bundeswehr im Inland mit zivilen Stellen zusammenarbeiten, um neben der Verteidigung zusätzlich bei der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit zu unterstützen. In diesem Kontext relevant sind zudem das **Wehrpflichtgesetz (WPflG)**, welches die Wehrpflicht und die Einberufung von Reservisten regelt, sowie das **Soldatengesetz (SG)**, das die Rechte und Pflichten der Soldaten thematisiert. Weiterhin können bestimmte Betriebe und Einrichtungen verpflichtet werden, nach den bestehenden **Sicherstellungs- und Vorsorgegesetzen** Vorsorgemaßnahmen zu treffen und im Einsatzfall eine fortgesetzte Leistungsfähigkeit sicherzustellen.[1] Diesen Gesetzen kommt eine besondere Bedeutung als „Reserve des Rechts“ zu, die mittels Beschlusses der

Alle Quellen und Erläuterungen finden Sie auf Seite 65 ↗.

Bundesregierung (Vorsorgegesetze) im Falle einer Versorgungskrise beziehungsweise mit Feststellung des Verteidigungsfalls (Sicherstellungsgesetze) aktiviert werden kann.[2] Hierbei ist im Besonderen die Rolle des **Bundesleistungsgesetzes (BLG)** hervorzuheben, welches es seit seiner Einführung 1956 staatlichen Stellen bei nationalen Krisen oder im Verteidigungsfall ermöglichte, Ressourcen und Dienstleistungen von Unternehmen und Privatpersonen zu verpflichten. Zusätzlich regeln **Unabkömmlichkeitsverordnungen**, welche Personen im Katastrophenfall von entgegenstehenden Pflichten, etwa dem Wehrdienst, freigestellt werden können, um ihre Aufgaben im Katastrophenschutz wahrnehmen zu können. Zuletzt bildet **Art. 73 Abs. Nr.1 GG** das Fundament für die Gesetzgebungskompetenz des Bundes für die Gesamtverteidigung und begründet somit den entsprechenden Verfassungsauftrag. Gesamtverteidigung ist zudem Bündnisauftrag im Rahmen von NATO (und EU).

Bündnisverteidigung

Für die Bündnisverteidigung kommt im Spannungs- sowie Zustimmungsfall[3] **(Art. 80a GG)** neben **Art. 87a GG** noch zusätzlich **Art. 24 Abs GG** zum Tragen. Dies ermöglicht es Deutschland, sich einem System gegenseitiger kollektiver Sicherheit wie der NATO anzuschließen. Zusätzlich besagt **Art. 5** des **NATO-Vertrages,** dass Angriffe auf eine NATO-Partei als Angriff auf alle NATO-Partner angesehen werden. Auch unterhalb dieser Schwelle ist Deutschland an die Bestimmungen des **NATO-Vertrages** gebunden, welcher die Grundlagen für die NATO-Verteidigungsplanung und damit die Verteidigungs- und Abschreckungsfähigkeit der Bündnispartner in Friedenszeiten legt. Konkret heißt es dort in **Art. 3**: „Um die Ziele dieses Vertrags besser zu verwirklichen, werden die Parteien einzeln und gemeinsam durch ständige und wirksame Selbsthilfe und gegenseitige Unterstützung die eigene und die gemeinsame Widerstandskraft gegen bewaffnete Angriffe erhalten und fortentwickeln.[4]“ Hieraus leitet sich zudem die Verpflichtung zum Host Nation Support (HNS) ab, welcher festlegt, dass ein Gastland (Host Nation) alliierten Streitkräften bei deren Stationierung, Transit oder Operationen auf seinem Territorium Unterstützung gewährt. Diese kann nach Bedarf logistische, administrative und infrastrukturelle Ressourcen umfassen, etwa die Bereitstellung von Unterkünften, Treibstoffen, Verpflegung, medizinischer Versorgung und Transportmitteln.

Der Einsatz der Bundeswehr im Inland wird zentral durch das Territoriale Führungskommando der Bundeswehr (TerrFüKdo, ab 1. April 2025 Operatives Führungskommando der Bundeswehr [OpFüKdo]) geführt und koordiniert, welches alle Aufgaben im Inland inkludiert.[5] Dem TerrFüKdo beziehungsweise OpFüKdo sind 16 Landeskommandos unterstellt, die als direkte Ansprechstellen für Unterstützungsleistungen oder Amtshilfen dienen und in jedem Bundesland vertreten sind. Die Landeskommandos spielen eine entscheidende Rolle in der Umsetzung der NATO-Verpflichtungen auf regionaler Ebene und fungieren als Schnittstellen zwischen der Bundeswehr und den zivilen Behörden der Bundesländer. Diese Kommandos sind dafür verantwortlich, die lokalen Bedingungen und Bedürfnisse der Bundesländer in die übergeordneten militärischen Planungen einzubringen, wodurch eine passgenaue Unterstützung im Falle von Bündnisverteidigungsmaßnahmen gewährleistet wird.

Abschließend beschreibt die **Rahmenrichtlinie für die Gesamtverteidigung (RRGV)** die notwendigen Maßnahmen und Strukturen, um die Unabhängigkeit und Souveränität Deutschlands in Krisen- und Konfliktzeiten zu sichern.

4.1.3 Hybride Bedrohungslagen

Im Gegensatz zu Bedrohungen der inneren und äußeren Sicherheit handelt es sich bei Hybriden Bedrohungslagen um ein vergleichsweise junges Phänomen, für welches bislang keine allgemeingültige Definition besteht. Oberst Dr. Johann Schmid vom Zentrum für Militärgeschichte und Sozialwissenschaften der Bundeswehr beschreibt diese prominent als „eine spezifische

Alle Quellen und Erläuterungen finden Sie auf Seite 65 ↗.

Form der Kriegsführung, die das Gefechtsfeld horizontal entgrenzt und eine Entscheidung insbesondere auch auf nicht-militärischen Handlungsfeldern anstrebt, die in den Grauzonen von Schnittstellen operiert und damit strategische Ambiguität erzeugt und die den Gegner durch unorthodoxe Mittel- und Methodenkombinationen herausfordert".[6] Vergleichbare Definitionen wurden durch Joint Research Center der Europäischen Kommission, US-amerikanischen Argonne National Laboratory sowie die NATO formuliert.[7][8][9] All diesen ist gemein, dass stets von einer Kombination konventioneller und unkonventioneller Mittel zur verdeckten Erreichung eines vordefinierten, illegitimen Ziels in einem fremden Staat ausgegangen wird.[10] Bedingt durch diesen breiten Definitionsraum lassen sich darunter eine Vielzahl möglicher Bedrohungslagen subsummieren, die jede für sich bereits eine intensivierte ZMZ erforderlich machen. Die nachfolgenden vier Fallbeispiele verdeutlichen diese Vielfalt exemplarisch:

Beispiele hybrider Kriegführung

Cyberangriff auf kritische Infrastruktur mit gesamtgesellschaftlicher beziehungsweise wirtschaftlicher Bedeutung

Ein koordinierter Cyberangriff auf das deutsche Stromnetz durch unbekannte Akteure, der zu großflächigen Stromausfällen führt. Hierbei werden technische Mittel (Cyberangriff) mit dem Ziel eingesetzt, die öffentliche Ordnung und das Vertrauen in staatliche Institutionen zu destabilisieren.

Desinformationskampagne während einer Wahl

Die massenhafte Verbreitung von gefälschten Nachrichten und manipulativen Inhalten in sozialen Medien mit dem Ziel, einen Wahlausgang zu beeinflussen, dessen Legitimität zu untergraben und politische Instabilität zu erzeugen.

Unterstützung extremistischer Gruppen

Ein fremder Staat finanziert und unterstützt verdeckt extremistische Gruppen in Deutschland, die gewalttätige Proteste und Unruhen organisieren, um gesellschaftliche Spannungen zu verschärfen und das Vertrauen in die Sicherheitskräfte zu untergraben.

Sabotage/Spionage mit überregionaler Bedeutung

Über sicherheitskritischer Infrastruktur werden wiederholt Spionagedrohnen gesichtet, die absehbar einen Sabotageakt durch unbekannte Akteure vorbereiten und Schwachstellen für einen möglichen Konfliktfall auskundschaften.

Abgrenzung

Hybriden Bedrohungen ist gemein, dass ihnen im Gegensatz zum Katastrophenfall zumeist kein klar bestimmbares Einzelereignis zugrunde liegt sowie abgrenzend zum Landes- oder Bündnisverteidigungsfall die Schwelle zu einem offenen militärischen Konflikt (bislang) nicht überschritten wurde. Zugleich besteht jedoch ein erhebliches Bedrohungspotenzial für Wirtschaft und/oder Gesellschaft des betroffenen Landes, welchem durch die geltende Rechtslage im Friedenszustand nicht angemessen begegnet werden kann. Folglich handelt es sich bei einer Hybriden Bedrohungslage um ein Szenario, das bislang zwischen zwei Rechtszuständen verortet und juristisch nicht eigenständig durch den Gesetzgeber geregelt wurde.

Relevante Akteure

Auf Bundesebene koordiniert das Bundesministerium des Innern und für Heimat (BMI) den Umgang mit Hybriden Bedrohungslagen. Es arbeitet auf der Grundlage eines Beschlusses der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK) federführend an einem „Gemeinsamen Aktionsplan von Bund und Ländern gegen Desinformation und für eine wehrhafte Demokratie" zur langfristigen Koordinierung einer bundesweit einheitlichen

Alle Quellen und Erläuterungen finden Sie auf Seite 65 ↗.

Strategie.[11] Seit 2023 leitet das BMI Im Kontext des Ukrainekrieges außerdem eine ressortübergreifende Taskforce zur Bekämpfung Hybrider Bedrohungen mit einem Fokus auf Desinformationskampagnen.[12] Weiterhin steht es bei allen die innere und äußere Sicherheit betreffenden Belangen in engem Austausch mit den zuständigen Akteuren des Bundesministeriums der Verteidigung (BMVg), des Bundesamts für Verfassungsschutz (BfV), des Bundeskriminalamts (BKA) sowie des Bundesnachrichtendiensts (BND). Die genannten Stellen unterstützen das BMI auf Basis nachrichtendienstlicher Erkenntnisse, Ermittlungsarbeit und weitergehender Analysen bei der Einschätzung Hybrider Bedrohungslagen und sind daher von kritischer Bedeutung.

4.2 Erklärung einer Hybriden Bedrohungslage

Basierend auf dem derzeitigen Status quo, den Beschlüssen der IMK sowie dem Grundgesetz lässt sich in Friedenszeiten eine klare Zuständigkeit des BMI und damit in letzter Instanz der Bundesministerin oder des Bundesministers des Innern und für Heimat für die Erklärung einer Hybriden Bedrohungslage ableiten. Gleichwohl liegt es in deren vielfältiger Natur, dass die Erklärung einer solchen stets eine Ermessensentscheidung je nach Informationslage und absehbaren Auswirkungen darstellen dürfte. Diese Entscheidung gälte es, mittels fundierter Nachweise der deutschen Sicherheitsbehörden zu begründen und gegenüber gangbaren Alternativen abzuwägen. In Ermangelung einer gesetzlichen Regelung ginge eine solche Erklärung jedoch nicht mit einer erweiterten deutschen Handlungsfähigkeit einher. Mit Blick auf die sich verschärfenden geopolitischen Spannungen und zunehmenden Bedrohungen der deutschen Sicherheit besteht daher seitens des Gesetzgebers Handlungsbedarf. Insbesondere gilt es Klarheit zu schaffen, ob und falls ja, in welcher Form der Sonderzustand einer Hybriden Bedrohungslage eine eigene juristische Regelung erfordert, diese abgrenzend zu definieren sowie die Verantwortlichkeiten zu dessen Erklärung zu regeln. Letzteres ist für dessen reale Anwendung essenziell, um bestehenden Entscheidungsaversionen in der bundesdeutschen Verwaltung frühzeitig entgegenzuwirken.

4.3 Schlussfolgerung zu bestehenden Rechtslücken zur Regelung Hybrider Bedrohungslagen

Resultierend aus diesen Rahmenbedingungen leiten sich mehrere mögliche Handlungsoptionen zur rechtlichen Regelung Hybrider Bedrohungen ab. Eine Verfassungsänderung könnte theoretisch die umfassendste und eindeutigste Lösung bieten, um Hybride Bedrohungen rechtlich zu verankern und zu adressieren. Allerdings sind die Hürden für eine solche Änderung in Deutschland außerordentlich hoch, deren staatsrechtliche Implikationen schwer abzuschätzen und diese somit kaum praktikabel. Damit verbleiben zwei realistische Handlungsoptionen:

4.3.1 Option 1: Agieren innerhalb der geltenden Rechtslage

Das Agieren innerhalb der bestehenden Rechtslage stellt die aufwandsärmste Option dar, da es keinen unmittelbaren legislative Eingriff erfordert und die bestehenden gesetzlichen Grundlagen bei konsequenter Anwendung bereits gewisse Handlungsspielräume ermöglichen. Indes sind diese kleinteilig durch eine Vielzahl teils kaum bekannter Einzelgesetze geregelt. Eine eindeutige, spezifische Regelung für Hybride Bedrohungen besteht bislang nicht, was die Reaktionsfähigkeit der relevanten Akteure verlangsamt und eine intensivierte ZMZ verhindert. Sollte weiter in der geltenden Rechtslage agiert werden, so gälte es, die juristischen Spielräume bestehender Gesetze in einem eigenständigen Rechtsgutachten zu bündeln und bei Entscheidungsträgern durch geeignete Maßnahmen das Bewusstsein für deren Anwendbarkeit zu fördern.

Alle Quellen und Erläuterungen finden Sie auf Seite 65 ↗.

4.3.2 Option 2: Einfacher Gesetzesbeschluss

Die Einführung eines eigenständigen Gesetzes zur Regelung Hybrider Bedrohungen würde es ermöglichen, den bislang bestehenden rechtlichen Graubereich zu beseitigen und die Kompetenzverteilung zuständiger Stellen, etwa des BMI, des Bundesministeriums der Verteidigung (BMVg) und der deutschen Sicherheitsbehörden, in einem Eintrittsfall transparent zu regeln. Die exakten Bedarfslücken der bestehenden Gesetze gälte es auch hier vorab rechtssicher zu ergründen, um juristische Dopplungen zu vermeiden. Ein Gesetzesbeschluss zur Schließung identifizierter Lücken könnte mittels bestehender politischer Mehrheiten zügig durch den Bundestag und den Bundesrat gebracht werden und erfordert keine Änderung des Grundgesetzes. Er stellt damit eine praktikable und effektive Option dar, um die Effizienz deutscher Abwehrmaßnahmen zeitnah zu erhöhen, deren Koordinierung im Kontext der ZMZ zu verbessern sowie deren Reaktionszeit zu beschleunigen.

4.4 Handlungsnotwendigkeiten

In Anbetracht der Analyse lässt sich konstatieren, dass der in Deutschland geltende Rechtsrahmen bereits umfangreiche Handlungsspielräume eröffnet, jedoch durch seine Komplexität und in Teilen Antiquität dessen Ausschöpfung erschwert. Vor diesem Hintergrund ist ein einfacher Gesetzesbeschluss zu empfehlen, um für den Ernstfall einer Hybriden Bedrohungslage vorzusorgen. Diese Option bietet einen ausgewogenen Ansatz zwischen Praktikabilität und Wirksamkeit, ohne die Unsicherheiten rechtlicher Grauzonen oder die hohen Hürden und potenziellen Risiken einer Verfassungsänderung in Kauf nehmen zu müssen. Ein eindeutig anwendbarer, juristisch solide verankerter Rechtsrahmen ist daher als unabdingbar zu betrachten, um die Sicherheit und Stabilität Deutschlands angesichts der zunehmenden Hybriden Bedrohungen zu gewährleisten und die politisch relevanten, gegenüber der NATO eingegangenen Verpflichtungen Deutschlands zu bedienen. Um seine volle Wirksamkeit zu entfalten, bedarf ein solcher Rechtsrahmen jedoch zugleich der Kohärenz der mit ihm einhergehenden politischen Maßnahmen und Ressourcenallokation, ohne welche auch die umfassendste legislative Regelung hinter den in sie gesetzten Erwartungen zurückbleiben muss.

Alle Quellen und Erläuterungen finden Sie auf Seite 65 ↗.

5 Zivil-Militärische Zusammenarbeit 4.0 im militärischen Krisenfall (Ausgangsszenario als Betrachtungsgrundlage)

Zeitpunkt: Ende Mai 2030

Mit Blick auf das Thema dieses GRÜNBUCHES, die Zivil-Militärische Zusammenarbeit im militärischen Krisenfall der Zukunft, wird als Beispiel das folgende Bild von Ereignissen gezeichnet, die sich so oder so ähnlich in zeitlicher Nähe abspielen könnten. Es dient als Grundlage und Einordnung der in den Folgeschritten beschriebenen vier exemplarischen Handlungsfeldern der ZMZ. Das Szenario bewegt sich nach Ablauf und Umfang bewusst nicht am oberen Ende des Möglichen, sondern beschreibt einen eher geringen Truppenumfang von unter 100.000 Soldatinnen und Soldaten mit dem entsprechenden Großgerät und Material.

Eine Entscheidung der NATO und ihrer Mitgliedsstaaten zu einem „All-in“ des NATO New Force Model, welches auf dem Gipfel in Madrid 2022 im Rahmen des neuen strategischen Konzeptes beschlossen wurde, würde den Einsatz von bis zu 800.000 Soldatinnen und Soldaten innerhalb von 180 Tagen bedeuten.

5.1 Ausgangssituation

Europa um das Jahr 2029. Die aktive Phase des Krieges in der Ukraine konnte vor wenigen Jahren beendet werden. Russland hält aber noch Teile des Staatsgebietes der Ukraine besetzt. Schwere Waffen wurden in Folge einer großen Friedenskonferenz unter Beteiligung Chinas von der Kontaktlinie abgezogen. Obgleich noch kein Friedensvertrag besteht, hat Russland wesentliche Truppenteile abgezogen, die Ukraine hat angefangen zu demobilisieren.

Die NATO-Staaten betrachten die aktuelleren Entwicklungen mit Sorge. Die Stärke und Entschlossenheit der Allianz haben sich aber grundsätzlich ausgezahlt. Der US-Präsident äußert öffentlich, seine Mission sei erledigt, nun könne er seine Soldaten zurück in die USA holen.

Russland äußert sich zufrieden. Der Westen habe de facto anerkannt, dass Russland zumindest Teile der Ukraine zustehe und werde auch einsehen, dass dies für die ganze Ukraine zutreffe. Dem internationalen Frieden zuliebe werde Russland zunächst nicht auf sein historisches Recht bestehen. Es erwarte nun die zügige Aufhebung aller Sanktionen und stehe als Lieferant von günstigem Gas und anderen Rohstoffen bereit. An der historischen Mission der Heimholung aller Russen in ein historisch legitimiertes russisches Großreich halte man fest. Schließlich erkenne man auch die legitimen Einflusszonen der USA, Chinas und Frankreichs an.

In Deutschland haben die letzten fünf Jahre einen Aufwuchs an zivilen und militärischen Fähigkeiten gebracht. Allerdings sind der personelle Aufwuchs und die Ausstattung noch nicht so zügig vorangekommen wie erhofft. Dies betrifft bei der Bundeswehr zum Beispiel die Reserve/die Heimatschutzkräfte und weite Teile des Unterstützungsbereichs wie Logistik, Feldjäger und Sanitätskräfte.

5.2 Entwicklung

Bereits im **März 2030** beobachten westliche Nachrichtendienste eine massive Verlegung von russischen Heeres- und Luftverbänden nach Kaliningrad und Belarus. Russland erklärt dies als weitere Rückverlegung seiner Truppen der Ukraine-Front. Militärblogger erkennen allerdings auch Verbände und Einheiten, die eigentlich anderen Militärbezirken zuzuordnen sind.

Die NATO verlangt von Russland Erklärungen der Truppenbewegungen.

Anfang April führt Russland zusätzlich modernisierte Kräfte und frisches Gerät aus dem Osten in die Oblast Leningrad heran und lange Güterzüge bringen neue beziehungsweise modernisierte Panzer und Artillerie sowie Luftabwehrsysteme vom Typ S-500 in die Oblast Kaliningrad. Russland begründet dies mit der regulären Wiederaufnahme seiner militärischen Großübung „Zapad/Westen“, die während des Ukraine-Krieges unterbrochen war.

Aufgrund der großen Aufrüstung der NATO seit 2022 werde diese Übung benötigt, um die Einsatzbereitschaft gegen mögliche Aggressionen der NATO herzustellen. Belarus nimmt ebenfalls an der Übung teil.

Die russische Marine startet parallel eine länger angekündigte Großübung in der Ostsee mit Schwerpunkten vor Gotland und Bornholm.

Die baltischen Staaten, Polen sowie Schweden und Finnland vereinbaren am **15. April 2030**, gemeinsam ihre nationalen Alarmstufen anzuheben. Sie bitten in der NATO um Konsultationen unter Artikel 5 des NATO-Vertrages: „Die Parteien werden einander konsultieren, wenn nach Auffassung einer von ihnen die Unversehrtheit des Gebiets, die politische Unabhängigkeit oder die Sicherheit einer der Parteien bedroht ist." Zudem fordern sie eine erhöhte Alarmbereitschaft der NATO-Kräfte in der Region sowie Verstärkungen.

18. April 2030: Die Bundesregierung ist sich mit ihren Verbündeten in der NATO einig, dass Russland in dieser Situation eine echte Gefahr darstellt. Man will Entschlossenheit demonstrieren. Daher soll die NATO-Präsenz in der Region drastisch verstärkt werden. Insgesamt sollen Europäer und die USA jeweils mindestens eine volle Division ins Baltikum sowie nach West-Polen entsenden und zusätzlich Gerät und Munition nach Polen sowie die skandinavischen Staaten herangeführt werden. Die Maßnahmen sind von strategischer Kommunikation begleitet: Sie würden sofort beendet, sobald Russland seine Kräfte glaubwürdig zurückziehe.

18. April 2030: Russland warnt die NATO vor jeglicher Art der Konfrontation.

5.3 Maßnahmen

21. April 2030: Die Bundesregierung, der Bundestag und die NATO sind sich einig, dass kein Spannungsfall ausgerufen werden soll, um Russland keinen Vorwand für Eskalation zu liefern. Aber es soll ein sichtbares Zeichen der Entschlossenheit und Abschreckung gesetzt werden.

Die Bundeswehr aktiviert Reservisten und insbesondere den Heimatschutz und ist bei der Umsetzung ihrer eigenen Aufgaben und der Erfüllung des Host Nation Supports (HNS) auf massive zivile Unterstützung angewiesen und bittet vor allem die Organisationen des Bundes, die Länder und Kommunen um tatkräftige Unterstützung.

Anfang Mai 2030: Die Bundeswehr beginnt mit der Verlegung von ersten Teilen der 10. Panzerdivision nach Litauen. Anteile der Division Schnelle Kräfte werden teils per Luft verlegt. Teil der Verlegung sind niederländische Verbände, die aus ihrer Heimat dazustoßen, sowie Kräfte aus Kroatien und Norwegen. In der Summe werden dies etwa 30.000 Soldaten sein. Die NATO und die Luftwaffe verstärken die Überwachung des deutschen Luftraumes und jenes über der Ostflanke.

15. Mai 2030: Großbritannien, Kanada und Frankreich kündigen an, ihre Kräfte in Estland und Lettland, um rund 15.000 Personen aufzustocken und planen dafür im Laufe des Juni und Juli einen Transit von Material, Munition und Personen durch Deutschland.

16. Mai 2030: Die USA beginnen große Teile ihrer in Deutschland stationierten Kampfverbände, etwa 25.000 Personen, aus dem süddeutschen Raum in Richtung Polen zu verlegen. Zudem führen sie über deutsche Häfen größere Mengen an Material, Munition und zwei bis drei weitere Kampfbrigaden nach, die im Juni eintreffen sollen (je 8.000 Soldatinnen und Soldaten). Ein Großteil der Munition und des Gerätes soll dann direkt in Richtung Polen auf den Weg gebracht werden.

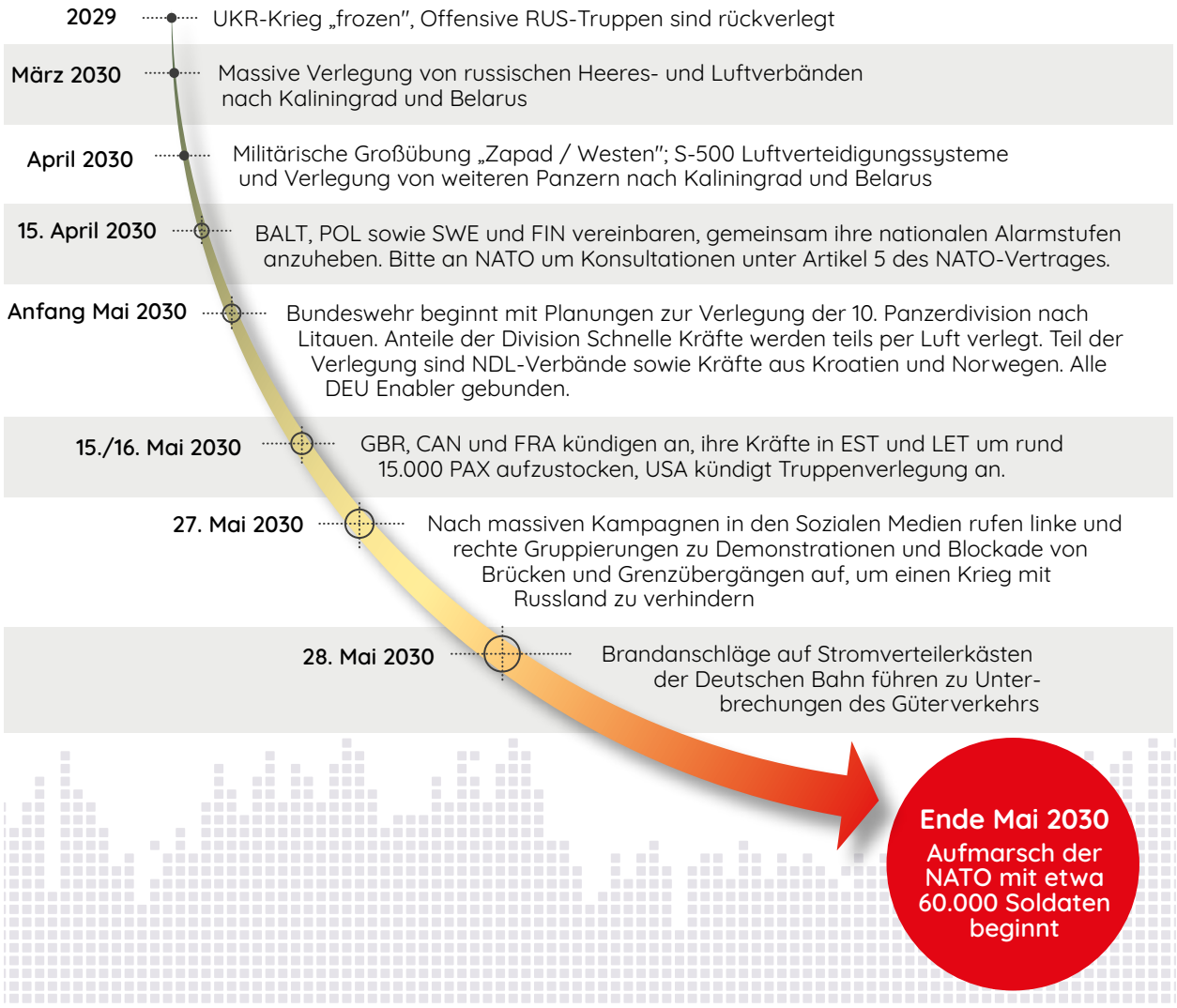

Abbildung 7: Szenar[13]

5.4 Lageverschärfende Ereignisse

27. Mai 2030: Im Internet steigt ein Informationsaufkommen, nachdem sich die NATO-Militärkonvois in Bewegung setzen, um das ukrainische Territorium gegenüber Russland abzusichern. Friedensaktivisten und NATO-Gegner von links und rechts rufen zu Demonstrationen und Blockaden von Brücken und Grenzübergängen auf, um einen Krieg mit Russland zu verhindern.

28. Mai 2030: Brandanschläge auf Stromverteilerkästen der Deutschen Bahn führen zu Unterbrechungen des Güterverkehrs, vor allem um Köln, Berlin und Oldenburg. Laut Bekennerschreiben einer unbekannten linksautonomen Gruppe war der Automobilexport das Ziel.

5.5 Zukunft

25. Juni 2030: Russland bezeichnet den NATO-Truppenaufbau von inzwischen gut 60.000 Personen im Baltikum und in Polen als „hysterisch und unverantwortlich". Er sei eine Gefährdung von internationalem Frieden und Sicherheit und stelle eine Bedrohung des russischen Hoheitsgebietes in Kaliningrad dar. Russland werde deshalb nach Beendigung seiner Übungsaktivitäten alle Truppenteile in der Region belassen.

30. Juni 2030: Die NATO beschließt daraufhin ihre abschreckenden Maßnahmen beizubehalten und plant dafür eine halbjährliche Rotation der Truppen und den Aufbau weiterer Logistik.

Alle Quellen und Erläuterungen finden Sie auf Seite 65 ↗.

6 Betrachtung ausgewählter Fallbeispiele

6.1 Unterstützung des Truppenaufmarsches

6.1.1 Ausgangssituation

Die angenommene Ausgangssituation sieht eine massive Verlegung von NATO-Verbänden ab Mai 2030 an die Ost-Flanke des Bündnisses mit Marschrouten durch die Bundesrepublik Deutschland in einem Gesamtumfang von rund 80.000 Soldatinnen und Soldaten mit entsprechendem Gerät, Material und Munition vor. Diese Aufgabe ist in einer Situation unterhalb des Spannungs- und Verteidigungsfalls, indes bereits unter dem Einfluss hybrider Bedrohungen und Störmaßnahmen zu bewältigen.

6.1.2 Host Nation Support (HNS)

Die notwendige Unterstützung dieses skizzierten Truppenaufmarsches ist im Rahmen von Host Nation Support (HNS) zu gewährleisten.

Grundsatz: Host Nation Support (HNS) spielt eine entscheidende Rolle für die militärische Bündnisfähigkeit und Abschreckung der NATO, insbesondere durch die Unterstützung ausländischer Streitkräfte auf deutschem Boden. Mit der „Zeitenwende“ geht ein Paradigmenwechsel einher, der HNS zu einer dringlicheren verpflichtenden Leistung werden lässt. Dies stellt neue Herausforderungen in Bezug auf Ressourcen und Finanzierung dar, erfordert aber auch dezentrale, pragmatische Lösungen auf lokaler Ebene, um die notwendige militärische Unterstützung effizient sicherzustellen.

Positionsbestimmung: Der Begriff Host Nation Support (HNS) beschreibt die Unterstützung ausländischer Streitkräfte durch das Gastland, wobei innerhalb der Bundeswehr zwischen drei wesentlichen Arten dieser Unterstützung differenziert wird:

- Erstens die Bereitstellung von Leistungen im Inland für ausländische Truppen
- Zweitens die Unterstützung eigener Truppen während ihres Transits durch andere Länder
- Drittens die Bereitstellung von Unterstützung in Einsatzgebieten

Deutschland nimmt dabei eine doppelte Rolle ein: Es fungiert nicht nur als Gastgeber für internationale Streitkräfte, sondern nutzt auch die Gastfreundschaft anderer Nationen, um unsere eigenen Soldatinnen und Soldaten in Auslandseinsätzen zu unterstützen.

Entwicklungen: Im Zuge des sicherheits- und geopolitischen Paradigmenwechsels seit dem Ende des Kalten Krieges hat sich die strategische Lage im Raum entscheidend verändert. Damals verlief die NATO-Außengrenze mitten durch Deutschland. Heute hingegen hat sich die Grenze weit nach Osten verschoben und erstreckt sich durch Skandinavien und Osteuropa, etwa 1.000 bis 2.000 Kilometer von Deutschland entfernt. Dies hat weitreichende Auswirkungen auf die Logistik und die strategischen Planungen der NATO. Die geografische Lage der neutralen Staaten Schweiz und Österreich führt dazu, dass militärische Verstärkungen zwangsläufig durch Deutschland geleitet werden. Mit der Erweiterung der NATO ist die Bedeutung verschiedener Achsen – neben der traditionellen West-Ost-Richtung auch die Nord-, Nordost- und Südost-Richtungen – gewachsen. Eine schnelle und effiziente Verlegung von Truppen ist – wie im Ausgangsszenar vorgesehen – heute entscheidender denn je, um bedrohten NATO-Mitgliedsstaaten rasch zur Hilfe eilen zu können. Dies ist ein Schlüsselelement erfolgreicher Abschreckung und damit wesentlich für den Schutz des gesamten Bündnisgebiets vor äußeren Bedrohungen.

Leistungsumfang und Herausforderungen: Die Durchführung strategischer Aufmärsche über große Distanzen stellt erhebliche logistische Herausforderungen dar. In der Regel wird der Transport von Personal, Material und Munition getrennt organisiert, um die Effizienz zu maximieren. Ein Beispiel dafür sind schwere Kettenfahrzeuge, die für das Gefechtsfeld optimiert sind: Diese Fahrzeuge würden bei einem langen

Marsch über Straßen nicht nur erhebliche Abnutzung an sich selbst, sondern auch an der Infrastruktur verursachen. Um diesen Problemen entgegenzuwirken, werden verschiedene Transportmittel kombiniert – Straße, Schiene, Luft und See –, wodurch der Aufmarsch sowohl zeitlich als auch ressourcentechnisch optimiert werden kann. Doch diese Vorgehensweise bringt ihre eigenen Herausforderungen mit sich, insbesondere die Notwendigkeit, Personal, Material und Munition am Zielort wieder zusammenzuführen, sowie den erhöhten Schutzbedarf während des Transports. Die Pläne der NATO sehen dabei vor, dass im Bündnisfall bis zu 800.000 Soldatinnen und Soldaten mit ihren Fahrzeugen von West nach Ost verlegt werden müssen.

Die konkreten Leistungen des HNS umfassen dabei eine breite Palette von Unterstützungsmaßnahmen, die in Verlegesituationen essenziell sind. Dazu zählen unter anderem die logistische Unterstützung durch Verpflegung, die Bereitstellung von Betriebsstoffen, Übernachtungs- und Abstellkapazitäten, die Unterstützung bei Wartung und Sicherung sowie die medizinische Versorgung. Bei groß angelegten militärischen Aufmärschen kommt eine weitere, nicht zu unterschätzende Aufgabe hinzu: die Verkehrslenkung und Gefahrenabwehr, insbesondere angesichts der wachsenden Bedrohung durch hybride Kriegsführung, wie sie sich bereits in der Ausgangslage durch Störungen realisiert. Die Sicherheit der Truppen während ihres Transits und die effektive Verwaltung des Verkehrsflusses sind in solchen Situationen von entscheidender Bedeutung, um die militärische Handlungsfähigkeit zu gewährleisten.

Historisch gesehen waren die Zuständigkeiten für HNS innerhalb der Bundeswehr auf verschiedene Führungsebenen sowie auf die Führungsgrundgebiete 3 (Durchführung) und 4 (Logistik) aufgeteilt. Diese Aufteilung führte jedoch oft zu Koordinationsproblemen und Unklarheiten in der Zuständigkeit. Um diese Herausforderungen zu überwinden, wurde im Operativen Führungskommando eine zentrale Koordinierungsstelle für HNS geschaffen, die alle relevanten Zuständigkeiten bündelt. Dieser Schritt war ein bedeutender Fortschritt in der Optimierung der HNS-Prozesse. Mit der Aufstellung des Operativen Führungskommandos der Bundeswehr wurde ein weiterer Meilenstein erreicht, indem die verschiedenen Zuständigkeiten und Abteilungen zu einer „HNS aus einer Hand"-Struktur zusammengeführt werden. Diese Neuorganisation orientiert sich an den bewährten NATO-Standards, insbesondere durch die Verortung von HNS in der Abteilung J4. Dies ermöglicht reibungslose Kooperationsbeziehungen und schafft klare Zuständigkeiten, die für eine effiziente Umsetzung von HNS unerlässlich sind.

Die aktuelle sicherheitspolitische Lage hat zudem einen Paradigmenwechsel im Bereich des Host Nation Supports eingeleitet. Bislang basierte die Bereitstellung von HNS-Leistungen auf einem freiwilligen, ressourcenabhängigen Prinzip, das vergleichbar mit der Amtshilfe im Inland war. Dieses Modell wird jedoch den aktuellen sicherheitspolitischen Herausforderungen nicht mehr gerecht. Angesichts der zunehmenden Bedrohungslage und der wachsenden Bedeutung einer schnellen Truppenverlegung drängt der Supreme Allied Commander Europe (SACEUR) der NATO auf eine verpflichtende Bereitstellung von HNS-Leistungen durch die Gastnationen. Diese strategische Neuausrichtung ist militärisch notwendig, um die Bündnisfähigkeit der NATO zu gewährleisten, bringt jedoch erhebliche Herausforderungen mit sich, insbesondere im Hinblick auf Ressourcen und Finanzierung.

Lösungsansätze: Eine mögliche Lösung für diese Herausforderungen liegt in der Entwicklung dezentraler Ansätze zur Bereitstellung von HNS-Leistungen.

6.1.3 Convoy Support Center (CSC)

Als Kernelemente im HNS-Leistungsspektrum fungieren so genannte Convoy Support Center (CSC). Sie sind im Grunde genommen Rast- und Sammelplätze für die mit Kraftfahrzeugen

marschierenden Truppen. Sowohl Mensch als auch Material bereiten sich dort mit logistischer Unterstützung durch Dritte auf ihre nächste Etappe vor und erhalten dort alles, was sie unterwegs im Spektrum Verpflegung/Betten/Treibstoff/Werkstatt benötigen.

Grundsätzlich können Convoy Support Center (CSC) auch in an der Marschroute liegenden militärischen Liegenschaften eingerichtet werden, weil dort die entsprechenden technischen und räumlichen Voraussetzungen ideal vorhanden sind. Die seit der Zeitenwende forcierte Integrierte Sicherheit im Rahmen gesamtstaatlicher Verteidigung verlangt jedoch zwingend effektive Redundanzen für bislang rein militärische angebotene Unterstützungsleistungen, die im Bereich der vierten Säule der KZV (Unterstützung der Streitkräfte) hoch wirksam abgebildet werden können. Für den Fall dringend benötigter CSC müssen daher jederzeit andere – zivile – Objekte mit vergleichbarem möglichen Wirkungspotenzial rechtzeitig identifiziert und betrieben werden, um zeitnah an jeder denkbaren Marschroute die erforderliche „Rastplatz-Unterstützung“ vollumfänglich leisten zu können. Für den Betrieb dieser CSC sind daher gerade zivile Behörden, Polizei und Blaulichtorganisationen sowie Vertragspartner aus der Wirtschaft erforderlich.

Die 11 Funktionalen Elemente
des Convoy Support Centers (CSC)

basierend auf einer Grafik des Bundesamtes für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr

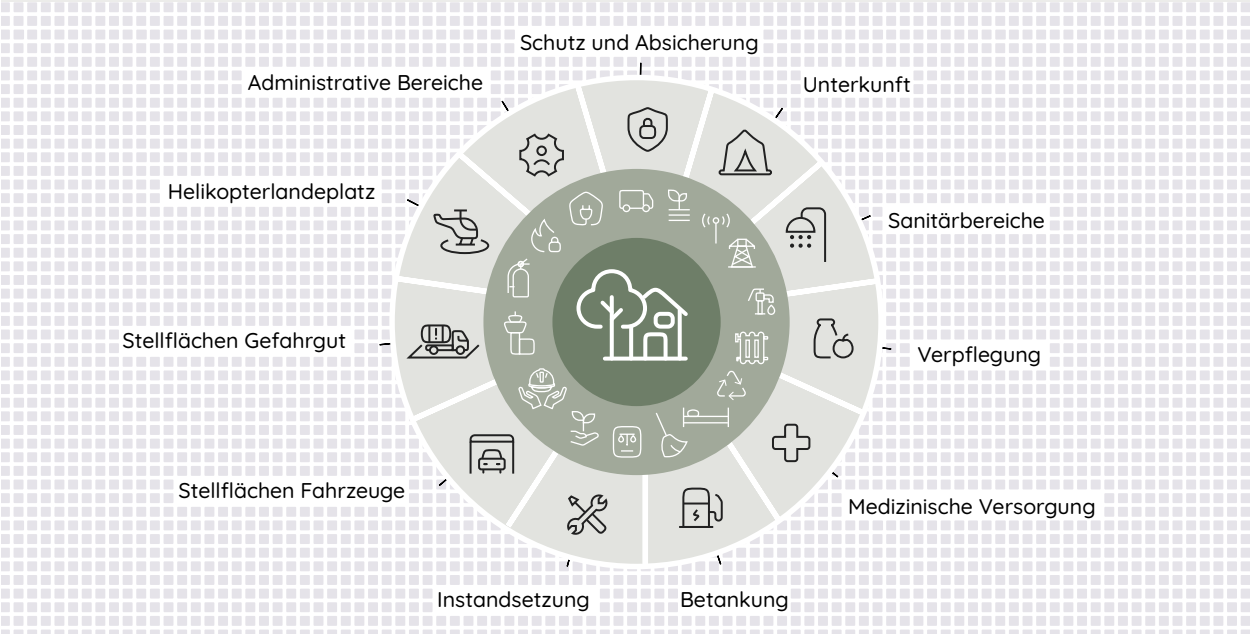

Abbildung 8: Convy Support Center

Praktisch jeder Landkreis in Deutschland hat das Potenzial, einen CSC zu errichten, der als lokaler Stützpunkt für Unterstützungsleistungen dienen kann. Es muss nicht immer eine aufwändige „Goldrandlösung“ sein; pragmatische und kosteneffiziente Lösungen, die auf den vorhandenen Ressourcen basieren, können ebenfalls effektiv sein. Hier sind insbesondere die Landrätinnen und Landräte entlang der Bewegungsachsen Straße und Schiene gefordert, zusammen mit den örtlichen Behörden zweckmäßige Lösungen zu entwickeln, um auf „CSC-Rastplätzen“ Unterstützung in Form von Unterbringung, medizinischer Versorgung, Sanitärwesen, Betankung, Instandsetzung und Abfallbeseitigung durchhaltefähig zu gewährleisten. Dies erfordert eine rechtzeitige und dauerhafte Sensibilisierung für die Bedeutung dieser Aufgabe

und eine enge Zusammenarbeit mit dem territorialen Netzwerk der Bundeswehr (hier den jeweiligen Landeskommandos und deren Bezirks- und Kreisverbindungskommandos), um Informationen und Planungen flächendeckend zu verbreiten. Auf dieser Ebene wird auch geklärt, wie beispielsweise notwendige Wach- und Sicherungsaufgaben für einen CSC auch bei „zivil geleiteter" Unterstützung durch militärische Kräfte abgesichert werden.

Die Herausforderungen der gesamten Bandbreite vom frühzeitigen Erkunden und Vorbereiten möglicher Standorte sowie Anbinden ziviler Logistikdienstleister und Abstimmungen mit allen Beteiligten bis zum realen Einrichten und Betreiben eines CSC gerade auch unter den Stressbedingungen bereits auftretender hybrider Bedrohungsszenarien und Wirkungsmöglichkeiten sind für zivile Behörden und Organisationen außerordentlich hoch. Gleichzeitig gilt es (und hier tritt ein Landkreis vor allem auch als politisch gewählte Exekutive auf), Organisationsmaßnahmen einer solchen Größenordnung der eigenen Bevölkerung zu vermitteln und entsprechende aufklärende Informationsarbeit (auch schon präventiv im Rahmen von Risikokommunikation) weit vorgelagert zu betreiben.

6.1.4 Leistungsverpflichtung im Rahmen der gesamtstaatlichen Verteidigung

Einer in vielen Fällen nicht mehr ausgeprägten Kenntnis und Bereitschaft zur eigenen zivilen Leistungsverpflichtung im Rahmen der gesamtstaatlichen Verteidigung muss daher frühzeitig mit einem sehr offensiven Informations- und Bildungsansatz begegnet werden, der zivile Körperschaften und Behörden, vor allem die Landkreise, zeitnah befähigt, die neu identifizierten Aufgaben- und Auftragsbereiche effektiv zu bearbeiten und die eigenen Strukturen im Bereich der Gefahrenabwehr und des Katastrophenschutzes im Sinne ganzheitlicher Zivilverteidigung zu optimieren.

Der Bedeutung der Zivil-Militärischen Zusammenarbeit (ZMZ) im Sinne hochwertiger moderner Interaktionen zum Zweck gesamtgesellschaftlicher Resilienzbefähigung im Allgemeinen und speziell zur Gewährleistung der Unterstützung der Streitkräfte kommt hier ein besonderer Stellenwert zu.

Landkreise und kreisfreie Städte mit deren Verwaltungsstäben nebst korrespondierenden Behörden und Organisationen mit Sicherheitsaufgaben (BOS) und den Betreibern Kritischer Infrastrukturen (KRITIS) sind daher aktiv kontinuierlich in entsprechende Übungs-, Aus- und Fortbildungsvorhaben einzubinden beziehungsweise entsprechende Angebote abzubilden, um die mit HNS verbundenen Aufgaben im Rahmen zivil-militärischer Interaktion wahrnehmen zu können.

Entsprechende CSC-Übungen im Rahmen „National Guardian" in Alsfeld (04/2024) und „Reliable Supporter 2024" in Rheine (10/2024) zeigten bereits die Fähigkeiten und Herausforderungen beim interaktiven zivil-militärischen Betrieb von CSC deutlich auf. Im Weiterbildungsformat „ZMZ" am Ausbildungsstützpunkt Bevölkerungsschutz Bad Sooden-Allendorf werden zudem seit 2022 entsprechende Szenarien mit dem Schwerpunkt ziviler Leistungserbringung für Landrätinnen und Landräte, Stäbe, BOS und Kreisverbindungskommandos (KVK) beübt und insbesondere die daraus entstehenden erweiterten Aufgabenverständnisse für zivile Verwaltungen und Multiplikatoren herausgearbeitet.

Entscheidend ist, wie in der vorgegebenen Lage zuverlässig, gerade auch mit zivilen Partnern, HNS-Leistungen wie einen CSC abgebildet werden können. Hierzu ist die frühzeitige Interaktion zwischen den verantwortlichen militärischen und zivilen Stellen erforderlich. Nur durch die frühzeitige Einbindung aller relevanten Akteure und die Entwicklung flexibler, lokaler Planungen kann Deutschland als Host Nation seine Rolle im NATO-Bündnis stärken und sicherstellen, dass im Ernstfall die notwendigen Ressourcen schnell und effektiv zur Verfügung stehen.

6.1.5 Handlungsnotwendigkeiten

- Landkreise und kreisfreie Städte sollten sich darauf einstellen, im Rahmen der ZMZ einen möglichen eigenen Unterstützungsanteil für den Bereich CSC im Krisenmanagement zu berücksichtigen und abzubilden. Dieses Spektrum umfasst das Erkunden möglicher CSC-Räume insbesondere im Bereich von Aufmarschrouten sowie vorab entwickelte und mit der Bundeswehr abgesprochene Konzepte für den Betrieb von CSC mit dem dafür notwendigen maximalen logistischen Leistungsportfolio.

- Die mit der Einrichtung und dem Betrieb eines CSC verbundenen Aufgaben, Auflagen und Folgen sind im Rahmen eines deutlich vorgelagerten, frühzeitigen Risikomanagements und entsprechender präventiver Risikokommunikation der Bevölkerung zu vermitteln.

- Die zivil-militärische Interaktion im Zusammenhang mit der Einrichtung und dem Betrieb eines CSC ist kontinuierlich in Aus-, Weiter- und Fortbildungen unter Beteiligung aller eingebundenen Partner (insbesondere zivile Verwaltung, BOS, Wirtschaft, Bundeswehr) zu beüben und zu verstetigen.

- Vorerkundungen möglicher Räume und administrative Festlegungen für eine derartige Planung und Unterstützung könnten auch im Sinne des Doppelnutzens des Zivilschutz- und Katastrophenhilfegesetzes (ZSKG) und der Strategie für einen modernen Bevölkerungsschutz umgekehrt auch wieder für das zivile Krisenmanagement oder den zivilen Katastrophenschutz von Nutzen sein.

6.2 Vorbereitung der Versorgung einer großen Anzahl Verwundeter bei gleichzeitiger Aufrechterhaltung des Gesundheitswesens für die Bevölkerung

Die zuverlässige Versorgung mit Leistungen des Gesundheitswesens ist für Militärangehörige und die Zivilbevölkerung/Zivilgesellschaft ein wichtiger Faktor für deren Moral und Resilienz in Krisen- und Konfliktfällen. Das Funktionieren des Gemeinwesens und des Staates wird daran gemessen. Kann die Funktionalität insbesondere für die Streitkräfte nicht nachgewiesen werden, wird die Abschreckung entscheidend geschwächt.

6.2.1 Vorbemerkung/Ausgangslage

Die im Rahmen einer auf Abschreckung ausgerichteten Verlegung von Einheiten der Bundeswehr und der NATO-Verbündeten, im Szenario genannte „Truppenverlegungen“, bedürfen zur Wirksamkeit eines Nachweises der Funktionalität aller darin enthaltenen – auch zivilen – Elemente. Dies gilt auch für die sanitätsdienstliche Absicherung aller Phasen eines solchen Einsatzes inklusive eines etwaigen Übergangs zu einem internationalen bewaffneten Konflikt. Die Wirksamkeit dieser Absicherung ist auch eine grundlegende Voraussetzung für die Motivation und das Vertrauen der eingesetzten Kräfte.

Gesamtverteidigung als Aufgabe der Zivilgesellschaft und der Bundeswehr bedeutet für alle Akteure im Gesundheitswesen, ihren Beitrag zu leisten und am Bedarf der Streitkräfte zu planen, so dass eine Umsetzung notwendiger Maßnahmen im Bedarfsfall unmittelbar erfolgen kann. Akteure des Gesundheitswesens im Sinne dieser Ausführungen sind beispielsweise Hilfsorganisationen im Katastrophenschutz und Rettungsdienst, ambulante Versorgungseinrichtungen, Apotheken, Arztpraxen oder die Kassenärztlichen Vereinigungen, Gesundheitsämter, Krankenhäuser und Rehabilitationseinrichtungen.

Eine rechtliche Besonderheit stellen die Hilfsorganisationen dar, die im „Gesetz über das Deutsche Rote Kreuz und andere freiwillige

Hilfsgesellschaften“ (2008) genannt sind. Dabei gilt, dass das DRK den Sanitätsdienst der Bundeswehr im Sinne des Artikels 26 des I. Genfer Abkommens unterstützt und Johanniter Unfallhilfe (JUH) und Malteser Hilfsdienst (MHD) zur Unterstützung des Sanitätsdienstes ermächtigt werden. Der Rechtsrahmen und die mit der Ermächtigung verbundenen Aufgaben sind jedoch nicht weiter konkretisiert worden, auch in der Konzeption Zivile Verteidigung (KZV) ist nur allgemein eine Unterstützung des Sanitätsdienstes durch die zivile Seite benannt. Die Konkretisierung der Aufgaben und der Rahmenbedingungen zu deren Erfüllung sind auch für die vorgenannten Hilfsorganisationen bisher jedoch nicht erfolgt. Es bestehen bisher keine Maßnahmen, die darauf abzielen, den Kräften den Schutzstatus der Sanitätskräfte nach Art. 26 I. Genfer Abkommen zukommen zu lassen. So fehlt es an der Unterstellung unter die militärischen Gesetze und Verordnungen sowie an der nötigen Notifikation für die Einsatzkräfte der Hilfsorganisationen, die im Sanitätsdienst der Bundeswehr mitwirken. Diese ist wesentlich, um den Einsatzkräften der ermächtigten Hilfsorganisationen, gerade in einem potenziell eskalierenden Geschehen im Einsatz für die Bundeswehr bestmögliche Fürsorge und völkerrechtlichen Schutz zu gewähren.

Für die nicht im Fokus des vorgenannten Gesetzes stehenden anderen Akteure (siehe oben) und die dort nicht aufgeführten Hilfsorganisationen, zum Beispiel Arbeiter-Samariter-Bund (ASB), Deutsche Lebens-Rettungs-Gesellschaft (DLRG) und andere Leistungserbringer im Rettungsdienst, Feuerwehren, Eigenbetriebe der Städte und Landkreise, private Anbieter., besteht das Problem, dass diese aktuell in Vorausplanungen nicht eingebunden sind und deren Rolle bislang auch nicht ansatzweise skizziert ist.

6.2.2 Szenare und mögliche Anforderungen der Bundeswehr im Rahmen der ZMZ

Auf militärischer Seite gibt es zum Beispiel im Rahmen der Arbeiten am Operationsplan Deutschland (OPLAN DEU) erste Überlegungen zu den entstehenden Bedarfen der Bundeswehr und der NATO-Partner.

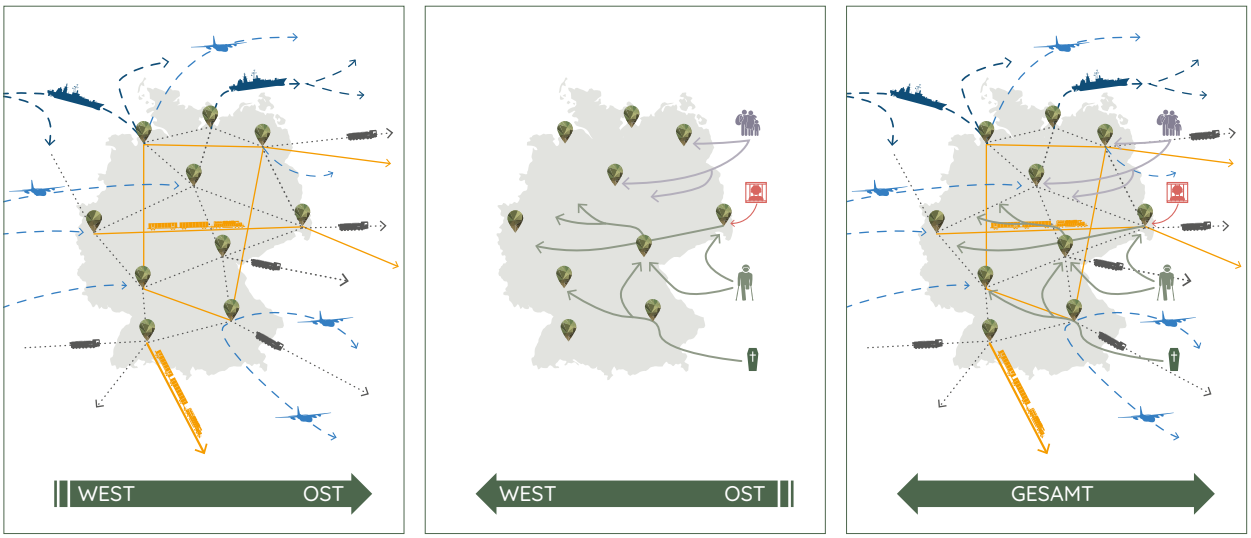

Abbildung 9: Drehscheibe Deutschland

In einem militärischen Krisenfall oder gar potenziellen Kriegsszenario wird es nicht nur Bewegungen in die eine, sondern in alle Richtungen geben (Flüchtlinge, Verwundete, Gefallene, Kriegsgefangene).

> *Zivilschutz, der überwiegend auf die Erfordernisse der militärischen Kriegsführung abgestimmt ist, hat diesen Namen nicht verdient.*
>
> *Das beste Argument dafür, grundsätzlich Frieden anzustreben, ist die lange Mängelliste im Bereich des Zivil- und Katastrophenschutzes im Inland!*
>
> *– Dr. André Hahn MdB*

Für den zivilen Sanitätsdienst ist im Rahmen Host Nation Support (HNS) etwa damit zu rechnen, dass für 60.000 Soldatinnen und Soldaten mit entsprechendem Gerät eine (hausärztliche) medizinische Versorgung sichergestellt werden muss.

Die im Falle einer militärischen Eskalation in Form von Kampfhandlungen darüber hinaus entstehenden Bedarfe der Bundeswehr sind der Zeitschrift Wehrmedizin und Wehrpharmazie (2/2023), Kohl M et al. S 38 ff.) zu entnehmen. Danach ist mit bis zu 1.000 Patientinnen und Patienten pro Tag zu rechnen, von denen 33,6 Prozent intensivpflichtig, 22 Prozent vermehrt pflegebedürftig und 44,4 Prozent leichter verletzt sind.[14] Die Autoren attestieren eine gravierende „hintere Transportlücke" für den strategischen Patiententransport (StratMedEvac) und kommen unter anderem zu dem Fazit, dass es in der konkreten operativen Planung ein Zusammenwirken von militärischen und zivilen Kräften erforderlich sei.

Weitere Einschätzungen finden sich in einem Artikel auf mdr.de vom 3. Mai 2024. Dietmar Pennig, Generalsekretär der Deutschen Gesellschaft für Orthopädie und Unfallchirurgie (DGOU), glaubt, dass derzeit die Bettenzahl auf militärischer Ebene innerhalb von 48 Stunden ausgeschöpft wäre. Innerhalb von zwei Tagen müssten verletzte Soldaten also auch in zivilen Krankenhäusern und Kliniken behandelt werden. Generalstabsarzt Norbert Weller betonte in diesem Zusammenhang, dass man auch hier vor einer Zeitenwende stünde, denn die europäischen Gesundheitssysteme mussten sich in den letzten 30 Jahren nicht mit der Versorgung mehrerer hundert Kriegsverletzter pro Tag beschäftigen. Es gehöre nicht zur Lebenswirklichkeit, daher sei eine umfassende Strategie erforderlich, was eine gesamtstaatliche Aufgabe sei. In diese Strategie müssen auch die jüngsten Erkenntnisse des Ukrainekrieges einfließen. So hat man zum Beispiel festgestellt, dass sich Verletzungsmuster verändert haben. Es gibt sehr viele Gefäß- und Amputationsverletzungen. Nun ist es aber so, dass in Deutschland die Versorgung von Kriegsverletzungen nicht Teil der chirurgischen Ausbildung ist. In den USA hingegen rotieren laut Pennig pro Jahr 50.000 Ärztinnen und Ärzte in die Militärkrankenhäuser. Dies wird staatlich finanziert, gefordert und gefördert. In Deutschland sei das – bislang – undenkbar. Um sich für das Szenario des Bündnisfalls zu wappnen, braucht es laut Weller starke Partner und etablierte Kooperationen. Es brauche ein belastbares Netzwerk sowie neue rechtliche Rahmenbedingungen für die Zusammenarbeit zwischen den Bundeswehrkliniken, den berufsgenossenschaftlichen Kliniken, den Unikliniken und den über 660 Kliniken des Trauma Netzwerkes Deutschland. Und nicht zuletzt braucht es auch einen Digitalisierungsschub.

Neben den zu erwartenden physischen Verletzungen und den dafür notwendigen Versorgungskapazitäten ist auch von einem erhöhten Bedarf an psychischen Behandlungskapazitäten auszugehen.

6.2.3 Vorhandene Potenziale der zivilen Notfallvorsorge

Für die oben genannten Bedarfe sind in der Katastrophen- und Zivilschutzplanung Einheiten der Hilfsorganisationen nicht vorgesehen. Dies ist auch sachlogisch, da die zivile Gesundheitsversorgung und der Katastrophenschutz vollumfänglich auf dem aktuellen Niveau aufrechtzuerhalten sind, somit auf Kräfte des Rettungsdienstes und des Katastrophenschutzes nicht zurückgegriffen werden kann. Diese sind durch ihren Kernauftrag gebunden und decken nach Anzahl und Qualifikation gerade den Bedarf. Eine Unterstützung durch die Hilfsorganisationen kann also nur durch den Einsatz freier Ressourcen und damit in begrenztem Umfang erfolgen.

Alle Quellen und Erläuterungen finden Sie auf Seite 65 ↗.

6.2.4 Ermittlung der Unterstützungsbedarfe des Sanitätsdienstes der Bundeswehr

Aus der bereits attestieren Lücke beim strategischen Patiententransport lässt sich der Bedarf der Bundeswehr ableiten. Deshalb bedarf es beim Transport erkrankter und verletzter Soldaten personeller, organisatorischer und materieller Unterstützung.

Bundeswehrkrankenhäuser sind aktuell in die Gesundheitsversorgung der Bevölkerung integriert und stehen auch für die Zivilgesellschaft für Behandlung und Pflege zur Verfügung. In einem Konfliktfall führen der Eigenbedarf der Bundeswehr und der Einsatz von (militärischem) Fachpersonal aus den Bundeswehrkrankenhäusern im Einsatzgebiet zu regionalen Versorgungseinschränkungen der Zivilbevölkerung.

Gleiches gilt für die derzeitige Einbindung der Bundeswehr in den zivilen Rettungsdienst; auch hier zeichnen sich im Einsatzfall der Bundeswehr Versorgungslücken ab.

Im Netzwerk der ZMZ-Partner muss ferner in die Betrachtung einfließen, dass Unterstützungskräfte des Katastrophen- beziehungsweise Zivilschutzes durch Bundeswehr und zivile Krankenhäuser, aber auch gegebenenfalls von Notunterkünften für Flüchtlinge angefordert und dort eingesetzt werden.

6.2.5 Einschätzung der Leistungsfähigkeit der Hilfsorganisationen und des Gesundheitswesens im Hinblick auf den Bedarf der Bundeswehr in Deutschland

Mit dem in der Corona-Pandemie etablierten und derzeit in der Verteilung von aus der Ukraine kommenden Patienten genutzten Transport- und Verteilsystem („Kleeblatt“) steht eine Konzeption zur Verfügung, die theoretisch auch als ziviles Unterstützungselement für die Bundeswehr für den qualifizierten Transport von erkrankten oder verletzten Bundeswehrangehörigen zum Einsatz kommen könnte. Da das Kleeblattsystem für geringe Patientenzahlen (Coronapandemie, aktuell Verwundete aus der Ukraine) entwickelt und eingesetzt wurde, ist eine Skalierbarkeit auf größere Patientenzahlen und -ströme nicht unmittelbar anzunehmen.

Für die Versorgung einer großen Anzahl Verletzter wird zwingend auf zivile Versorgungsstrukturen zurückgegriffen werden. Diese sind bereits aktuell sehr be- beziehungsweise überlastet. In der aktuell diskutierten Reform der Notfallversorgung ist eine Ausrichtung des Systems auf zusätzliche Patienten aus einem bewaffneten Konflikt nicht vorgesehen. Eine öffentliche Diskussion über eine daraus folgende Reduzierung des Versorgungsniveaus findet nicht statt, die Bevölkerung ist auf diese nötige Priorisierung nicht ausreichend vorbereitet. Wenn neben einem bewaffneten Konflikt zeitgleich andere, das System belastende Ereignisse (Pandemie, Naturkatastrophe) stattfinden, sind Versorgungseinschränkungen im Vergleich zum heute gewohnten Niveau nicht zu vermeiden.

In diesem Zusammenhang müssen auf jeden Fall auch größere Fluchtbewegungen aus den Nachbarländern des Konfliktes in die Betrachtung mit aufgenommen werden. Die Hilfsorganisationen wären dann gefordert, die Kommunen und Kreise massiv bei der Betreuung Schutzsuchender zu unterstützen.

Es fehlen verpflichtende Systeme, in Deutschland Überkapazitäten (freie Betten, freies Personal, freie Materialien) strukturell zu erfassen; vorhandene moderne digitale Instrumente zu Behandlungsnachweisen sind auf das betrachtete Szenario nicht ausgerichtet. Daher sind Pooling-/Sharing-Konzepte aktuell nicht umsetzbar.

Im Hinblick auf Rehabilitation scheint Deutschland mit mehr als 1.000 Reha-Einrichtungen zunächst gut aufgestellt. Allerdings sind diese hinsichtlich ihres Leistungsangebotes auf den alltäglichen Bedarf der Bevölkerung ausgerichtet und nicht auf die speziellen Anforderungen, die aus Verletzungsmustern verwundeter Soldatinnen und Soldaten resultieren.

6.2.6 Handlungsnotwendigkeiten

Die Handlungsfähigkeit des Zivilschutzes muss im zeitlichen Einklang mit den militärischen Bemühungen zur Kriegstüchtigkeit synchron erfolgen. Dies erfordert die unverzügliche Klärung der vorgenannten rechtlichen Fragestellungen, die Erstellung erforderlicher Konzeptionen und Planungen sowie der Durchführung gemeinsamer Ausbildungen und Übungen.

Daher ergeben sich aus den oben aufgeführten Analysen folgende Handlungsnotwendigkeiten:

Personal-/Materialverfügungen

Schaffung materieller Ressourcen (vor allem Material, Fahrzeuge, Medikamente und Medikalprodukte) zur Sicherstellung der sanitätsdienstlichen und hausärztlichen Versorgung im Rahmen HNS und für den strategischen Verwundetentransport in Bund-Länder offenen Arbeitsgruppen unter Beteiligung der Bundeswehr und der Hilfsorganisationen.

Schaffung zusätzlicher Personalkapazitäten

Nötige zusätzliche Kapazitäten sind zu schaffen. Bei der weiteren Ausgestaltung des „Auswahlwehrdienstes“ muss darauf geachtet werden, dass eine Möglichkeit eines Engagements bei den Hilfsorganisationen im Zivil- und Katastrophenschutz ausgewiesen und eine mehrjährige, an die Dauer des Wehrdienstes angepasste Dienstzeit für reine Zivil-/Katastrophenschutzaufgaben zur Deckung des Personalbedarfs ermöglicht wird. Zudem müssen entsprechende Bedarfsdeckungsmöglichkeiten nach den Sicherstellungsgesetzen eröffnet werden.

Transportkapazitäten

Die Hilfsorganisationen müssen zusammen mit den Streitkräften den personellen (quantitativ und nach Festlegung eines Versorgungsniveaus auch qualitativen) und materiellen (Fahrzeuge, medizinisches Material und Medikamente) Bedarf definieren der für die Convoy Support Center (CSC) sowie den strategischen Verwundetentransport, insbesondere für die Anschlusstransporte in Deutschland, festlegen. Zudem ist zu prüfen, ob im Rahmen des strategischen Patiententransportes auch die Weiterverlegungen nach erster Akutversorgung (Sekundärtransporte) und zu Rehabilitationseinrichtungen zu berücksichtigen sind.

Lagebild

Zur Erlangung eines aktuellen Lagebildes muss eine detaillierte Erfassung und Aktualisierung der vorhandenen Kapazitäten der zivilen Gesundheitsversorgung sowie der benötigten Unterstützungsbedarfe in digitaler Form auf einer gemeinsamen Plattform, idealerweise im geforderten digitalen Lagebild, erfolgen.

Patientenzuweisung/Übergabeorte

Um die Planungssicherheit für die Zielkliniken zu erhöhen und die Patientenverteilung verlässlich zu gestalten, ist ein Zuweisungssystem basierend auf der Leistungsfähigkeit der Kliniken zu präferieren. Vorteil eines solchen Systems sind die geringeren Abstimmungsaufwände im Verteilprozess, weil eine statische Vorabverteilung möglich ist. Ergänzend wäre die Übertragung des Regionalprinzips der Kleeblattregionen, regionale Transportorganisation und die Einrichtung von regionalen (zivil-militärischen) Verteilzentren zu fordern.

Übergabeorte der Patienten (Bahnhöfe/Flughäfen) sind in die Erfassung Kritischer Infrastrukturen (KRITIS) und die Liste „Objekte besonderer Bedeutung“ aufzunehmen und vor Sabotageakten und Angriffen zu schützen.

Die weitere Planung und Umsetzung sowie die Aufwuchsfähigkeit der Strukturen muss im Rahmen der Gesetzgebung zur Gesundheitssicherstellung und in der Gesetzgebung zu Gesundheitsreformen erfolgen.

Einschränkungen im Krankenhauswesen und dem Rettungsdienst, die sich aus der im Einsatzfall reduzierten Verfügbarkeit der Bundeswehr ergeben, sind von den Fachbehörden zu

prüfen und so zu beplanen, dass Kompensationsmaßnahmen in kürzester Zeit wirksam umgesetzt werden können.

Versorgungsniveau der Bevölkerung

Die Prüfung, ob und unter welchen Bedingungen das bestehende allgemeine Versorgungsniveau im Gesundheitswesen aufrechterhalten werden kann und welche zusätzlichen Kapazitäten ergänzt werden müssen, muss zeitnah erfolgen. Dabei können Simulationen Entscheidungshilfen bieten, mit denen unterschiedliche Szenarien betrachtet werden können. Basis dafür sind die Erstellung respektive der Ausbau des digitalen Gesundheitsatlasses. Zu prüfen ist eine Einbindung der Apotheken in die Erstversorgung wie bereits während der Corona-Pandemie für Impfungen geschehen.

Soweit Umsetzungen und Maßnahmen gewählt werden, die zu einer Einschränkung des Versorgungsniveaus führen oder die Qualität der medizinischen Versorgung absenken, ist eine Kommunikationsstrategie erforderlich, die die Maßnahmen der Bevölkerung erklären und das Gesundheitssystem durch Fehlinanspruchnahme nicht zusätzlich belasten. Ferner könnten KI-gestützte Systeme, beispielsweise ein Chatbot für Erkrankte, die Patienten bei der Entscheidung unterstützen, eine Behandlungsreinrichtung aufzusuchen oder nicht.

Erarbeitung des Unterstützungsbedarfes der Bundeswehr und deren Umsetzungsvoraussetzungen

Es bedarf der Festlegung erforderlicher Unterstützungsbedarfe nach Art und Umfang. Die rechtlichen und fiskalischen Voraussetzungen sind im Hinblick auf die Besonderheit der Mitwirkung im Sanitätsdienst anzupassen beziehungsweise zu schaffen, um dann die notwendigen organisatorischen und personellen Maßnahmen für deren Sicherstellung treffen zu können.

Durch die Bundeswehr gilt es zu definieren, welche konkreten Bedarfe hinsichtlich

- des strategischen Patiententransportes bestehen (Rückführung von Patienten aus dem Einsatzland nach Deutschland),
- der Verteilorganisation dieser Patienten auf Einrichtungen der Bundeswehr und des zivilen Gesundheitswesens in Deutschland und
- des personellen Unterstützungsbedarfes in den Einrichtungen der Bundeswehr

entstehen.

Darüber hinaus ist zu ermitteln, welche sanitätsdienstlichen („hausärztlichen“) Leistungen im Rahmen des Host Nation Supports (HNS) voraussichtlich zu erbringen sind. Je nach örtlicher Zuständigkeit sollten auf Basis dieser Angaben die Kassenärztlichen Vereinigungen und die Hilfsorganisationen zusammen mit der Bundeswehr eine Detailplanung vornehmen.

Rehabilitationsversorgung für Soldatinnen und Soldaten

Bei den angenommenen Verletztenzahlen von Soldatinnen und Soldaten bedarf es der Anpassung der Anzahl der zur Verfügung stehenden, geeigneten Plätze zur Rehabilitation. Die Anpassung muss auch durch Weiterbildung des dortigen Personals erfolgen. Zudem sind geänderte, auf das Rehabilitationsziel ausgerichtete Verfahren einzuführen. Auch sind Erhebungen und Simulationen dazu vorzunehmen, welche medizinischen Hilfsmittel voraussichtlich benötigt werden, und eine Marktsondierung durchzuführen, um gegebenenfalls die Kapazitäten/Verfügbarkeiten bei den Herstellern zu erhöhen.

Rechtliche Stellung der Hilfsorganisationen und ihrer Kräfte

Die rechtlichen Möglichkeiten zur Erfüllung der Vorgaben des I. Genfer Abkommens auf nationaler Ebene sind zu prüfen und umzusetzen.

Zudem muss geklärt werden, auf welcher rechtlichen Basis eine Beauftragung der Hilfsorganisationen erfolgen kann und unter wel-

chen Rahmenbedingungen die Abstellung der Kräfte erfolgen soll. Hier ist besonders zu betrachten, dass nach den Grundprinzipien des Zivilschutzes auf die ehrenamtlichen Hilfeleistungspotenziale zurückgegriffen werden soll und hauptamtliche Kräfte lediglich zur Verstärkung des Systems vorgesehen sind. Es ist daher zu klären, unter welchen Bedingungen gegebenenfalls Hilfsorganisationen im Auftrag der Bundesrepublik eigenständig ehrenamtliche Helfer für Unterstützungseinsätze alarmieren dürfen und wie Verdienstausfälle und sozialversicherungsrechtliche Fragen geregelt werden (zum Beispiel Lohn- und Gehaltszahlungen, Aufwandsentschädigung, Krankenversicherung sowie Haftungsfragen) oder aber, ob ein hauptamtlicher Personalpool aufgebaut und finanziert wird. Mögliche Lösungsansätze dazu bieten das Amtshilfeverfahren oder öffentlich-rechtlichen Verträge.

6.3 Aufrechterhaltung der öffentlichen Sicherheit und Ordnung

6.3.1 Verfassungsschutz – Ausgangssituation

Die Aufgabe des Verfassungsschutzes ist gemäß § 3 Abs. 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG) die Sammlung und Auswertung von Informationen:

Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben,

2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht,

3. Bestrebungen im Geltungsbereich dieses Gesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,

4. Bestrebungen im Geltungsbereich dieses Gesetzes, die gegen den Gedanken der Völkerverständigung (Art. 9 Abs. 2 Grundgesetz), insbesondere gegen das friedliche Zusammenleben der Völker (Art. 26 Abs. 1 GG) gerichtet sind.

Beispielhaft hierfür sind Arbeitsfelder des Landesamtes für Verfassungsschutz (LfV) Hamburg zu nennen: Islamismus, Rechts- und Linksextremismus, extremistische Bestrebungen von Gruppierungen mit Auslandsbezug, die Scientology-Organisation sowie die Spionagetätigkeit fremder Nachrichtendienste einschließlich Cyberspionage. Weiterhin werden im Phänomenbereich des verschwörungsideologischen Extremismus Delegitimierer, Reichsbürger und Selbstverwalter zusammengefasst. Darüber hinaus zählen der Geheim- und Sabotageschutz zu den weiteren Aufgaben des LfV Hamburg.

Information staatlicher Stellen

Der Verfassungsschutz wertet die mit offenen oder nachrichtendienstlichen Mitteln gewonnenen Erkenntnisse aus und informiert im Rahmen seiner gesetzlich festgelegten Aufgaben über entsprechende Gefahren (siehe beispielhaft § 4 Abs. 1 HmbVerfSchG). Dazu zählt in Hamburg die Informationsverpflichtung gegenüber dem Senat, weiteren staatlichen Stellen sowie der Öffentlichkeit.

Information der Öffentlichkeit

Ein breit geführter gesellschaftlicher Diskurs über die Gefahren extremistischer Bestrebungen sowie eine erhöhte Sensibilität aufgeklärter Bürgerinnen und Bürger angesichts potenzieller Bedrohungen sind essenzielle Bestandteile einer wehrhaften Demokratie.

In den Kontext dieses Konzeptes der streitbaren Demokratie und der darin festgelegten Aufgabe des Verfassungsschutzes als Frühwarnsystem ist die Öffentlichkeitsarbeit einzuordnen. Austausch und Kommunikation erfolgen dabei über eine Vielzahl von Kanälen. Dies sind unter anderem:

- Der jährliche Verfassungsschutzbericht
- Verschiedene Publikationen in klassischen und digitalen Kanälen
- Informations- und Diskussionsveranstaltungen
- Ausstellungen und Symposien
- Vorträge

Die Öffentlichkeitsarbeit der Cyberspionageabwehr mittels Flyer und Broschüren sowie im Internet ist eine gemeinsame Aufgabe des Verfassungsschutzverbundes. Zentrale Veröffentlichungsstellen sind die Homepage des BfV sowie das Portal der Initiative Wirtschaftsschutz.

Die **Cyberspionageabwehr** wirkt bei der Geheimschutzbetreuung des Bundes mit. Sie ist Ansprechpartner für die Unternehmen, bei denen es sich um geheimschutzbetreute Unternehmen (VS-Auftragnehmer) handelt. Die Mitwirkung beinhaltet insbesondere

- die Kontaktpflege und den Aufbau einer Vertrauensbeziehung,
- die Sensibilisierung der ermächtigten Personen,
- die Beratung bei konkreten Fragestellungen, die Unterstützung bei Sicherheits- oder Cybervorfällen.

Neben den VS-Auftragnehmern des Bundes betreuen in der Regel die Verfassungsschutzbehörden der Länder weitere Unternehmen. Dies ist der Fall bei KRITIS-Unternehmen oder bei Unternehmen, die sich wegen unterschiedlichster Anliegen an den Fachbereich gewandt haben.

6.3.2 Hybride Bedrohungen – Abwehrmaßnahmen und die Rolle des Verfassungsschutzes

Unter dem Oberbegriff Hybride Bedrohungen versteht man verschiedene Formen illegitimer Einflussnahme durch ausländische Akteure, die strategische Ziele insbesondere politischer, aber auch wirtschaftlicher Art verfolgen und anderen Staaten schaden wollen. Zu den hybriden Instrumenten der Akteure zählen etwa Desinformation, Cyberangriffe oder (Wirtschafts-) Spionage.

Seit Beginn des russischen Angriffskriegs gegen die Ukraine hat sich die Hybride Bedrohungslage in Deutschland noch einmal verschärft. Ziel Hybrider Bedrohungen sind alle politischen und gesellschaftlichen Ebenen.

Hybride Bedrohungen charakterisieren sich dadurch, dass grundsätzlich alles als Instrument eingesetzt werden kann. Die Zuordnung (Attributierung) zu einem Akteur ist oft nur schwer möglich.

Zur Abwehr Hybrider Bedrohungen ist ein möglichst breiter gesamtstaatlicher und gesamtgesellschaftlicher Ansatz notwendig.

Struktur

Im Fall eines beispielsweise durch hybride Einflussnahme bevorstehenden militärischen Krisenfalls, der Bezüge zum Zuständigkeitsbereich des Verfassungsschutzverbundes aufweist, greift ein **Konzept zur Bearbeitung von Besonderen Lagen**, das die Zusammenarbeit zwischen dem Bundesamt und den Ländern regelt.

Im Falle eines bevorstehenden militärischen Krisenfalls ist die **eigene Arbeitsfähigkeit** ebenfalls sicherzustellen.

Hier geht es um die Aufstellung etwaiger Dienstpläne/Notfallpläne, um die Erreichbarkeit, Verpflegung und Wasserversorgung der Mitarbeitenden, aber auch um Themen wie die Kommunikation innerhalb eines Landesamtes und im Verfassungsschutzverbund im Falle eines begrenzten kurzfristigen (deutlich unter 72 Stunden) Stromausfalls oder eines überregionalen sowie eines langfristigen Stromausfalls („Blackout"). Daneben sind beispielsweise die Verfügbarkeit von Benzin für Dienstfahrzeuge und das Vorhalten von Bargeldbeständen weitere Themen, die vorbereitet sein sollten.

Formen der Hybriden Bedrohung

Cyberangriffe

Ein Cyberangriff ist eine gezielte Attacke auf Computer oder Computernetzwerke. Beispiele für Auswirkungen von erfolgreichen Cyberangriffen sind die Störung von Betriebsabläufen, der Abfluss von Informationen, die Verweigerung von Zugängen sowie die Manipulation, Beschädigung oder Zerstörung von Hardware, Daten, Netzwerken oder technischen Systemen.

Fremde Nachrichtendienste nutzen Cyberangriffe teilweise in großem Umfang mit der Absicht, unbefugt an Informationen zu gelangen. Die hierzu veranlassten und gesteuerten Cyberangriffe stellen aufgrund ihrer Qualität und ihres Umfangs eine erhebliche Gefahr für das jeweilige Angriffsziel dar, das in der Regel zuvor anhand der politischen Vorgaben der eigenen Regierung ausgewählt wird.

Neben Spionageaktivitäten können Cyberangriffe auch zur Vorbereitung von Sabotageakten genutzt werden. Hat ein Angreifer erst einmal Zugriff auf ein IT-System erlangt, kann er dort ungehindert eine Vielzahl an Aktionen durchführen und damit auch die Verfügbarkeit des Zielsystems beeinträchtigen.

Beispiel

Methoden, durch die die Angreifenden in ein System eindringen, um dort Schadsoftware installieren zu können (sogenannte Angriffsvektoren).

Die im Opfersystem vorhandenen Sicherheitslücken bestimmen über den Erfolg des genutzten Angriffsvektors. Der am häufigsten verwendete Angriffsvektor für Cyberangriffe bildet (Spear-)Phishing. Hier erhält der Adressat eine vermeintlich authentische E-Mail, der zum Beispiel ein Dokument als Anhang beigefügt wurde oder die über einen Hyperlink auf eine Website verweist. Das Öffnen des Anhangs oder der Besuch der Website löst dann den ersten Schritt der Infektion mit einer Schadsoftware aus.

Abwehrmaßnahmen und Rolle des Verfassungsschutzes:

- Die Detektion von Cyberangriffen
- Die Attribution (Zuordnung) dieser Angriffe zu einem Staat, einer APT-Gruppierung (Advanced Persistent Threat) oder die Benennung beteiligter Personen an einem konkreten Cyberangriff
- Die Cyberabwehr informiert über mögliche Angriffe und veröffentlicht technische Indikatoren (Indicators of Compromise). Anlassbezogen werden durch die Cyberabwehr des Bundesamts für Verfassungsschutz (BfV) Warnhinweise wie beispielsweise in Form des „Cyber-Briefs" veröffentlicht.
- Weitere präventive Maßnahmen der Cyberabwehr bilden zudem Informationsveranstaltungen, Vorträge und Sensibilisierungsgespräche.

Einflussnahme und Desinformation

Eine Desinformationskampagne ist ausgehend davon eine über einen längeren Zeitraum mit einem definierten strategischen Ziel andauern-

de Aktion, die eine breite Wirkung beim Empfängerkreis entfalten soll. Urheber sind zumeist staatliche oder staatsnahe Akteure, die geplant und koordiniert zusammenwirken. Dabei können sowohl offene als auch verdeckte Mittel angewendet und auch kombiniert werden.

Desinformation kann in der Öffentlichkeitsarbeit von staatlichen Stellen (etwa Geheimdienst oder Militär), von politischen Parteien und Gruppen, von Lobbygruppen oder von Einzelpersonen vorkommen. Ziel ist Täuschung der Bevölkerung, Stimmungsmache oder Verwirrung des Gegners.

Bund und Länder arbeiten an einem gemeinsamen Aktionsplan unter Federführung des Bundesministeriums des Innern und für Heimat (BMI). Dieser Bericht soll Handlungsempfehlungen zur Verbesserung der frühzeitigen Erkennung von Desinformation, zur Stärkung der Strategischen Kommunikation, zu einer umfassenden Resilienzbildung und zu einer Intensivierung von Austausch und Forschung zum Thema Desinformation aufzeigen.

Zentrale strategische Ziele

- Strukturen und Zusammenarbeit zur frühzeitigen Erkennung, Analyse und Abwehr von Desinformation stärken beziehungsweise aufbauen
- Öffentlichkeitswirksame Aktivitäten und strategische Kommunikation im Umgang mit Desinformation und für eine wehrhafte Demokratie ausbauen
- Resilienzmaßnahmen gegen Desinformation fördern und Medien- und Nachrichtenkompetenz stärken
- Forschung zu Produzenten, zur Wirkung von Desinformation und zu möglichen Gegenmaßnahmen gezielt fördern

Antworten auf Hybride Bedrohungen liegen auch im zivilen Bereich. So können durch präventive politische Maßnahmen mögliche Angriffspunkte im Keim erstickt werden. Dazu zählt etwa eine vorausschauende Minderheiten-, Bildungs- und Wirtschaftspolitik, die zum Ziel hat, Unzufriedenheit bei den Menschen zu verhindern und somit ihre Anfälligkeit für Propaganda gering zu halten.

Beispiele

Versuch, das Vertrauen der Bevölkerung in die Stabilität und Handlungsfähigkeit der demokratischen Institutionen und Mechanismen verstärkt zu untergraben, die westliche Wertegemeinschaft zu diskreditieren und Bündnisse wie EU und NATO zu schwächen.

Das Vertrauen der Bevölkerung in die Stabilität und Integrität der Institutionen und Mechanismen unserer freiheitlichen Demokratie geschwächt, ihre Werte in Frage gestellt oder Zusammenschlüsse demokratischer Staaten wie die Europäische Union oder die NATO untergraben werden.

Abwehrmaßnahmen und Rolle des Verfassungsschutzes:

Um die gesamtstaatliche wie gesellschaftliche Resilienz gegen Desinformation und weitere Formen der illegitimen Einflussnahme zu fördern, tritt die Bundesregierung Desinformationsbemühungen strategisch sowie kommunikativ entgegen. Unterschiedliche Ressorts und Behörden arbeiten dafür eng zusammen. Das BfV unterstützt dabei als Frühwarnsystem das ganzheitliche Vorgehen der Bundesregierung gegen Desinformation und unzulässige ausländische Einflussnahme.

Wirtschaftsschutz

Schutz von Unternehmen vor Spionage-/Sabotageaktivitäten und Cyberspionage, mit dem Ziel, die Wirtschaft und Wissenschaft durch Informationen und Sensibilisierungen dabei zu unterstützen, sich effektiv gegen Spionageaktivitäten und extremistische Gefahren zu schützen.

Beispiele

Anwendungsfall 1
Das BfV übermittelt Hinweise auf die mögliche Betroffenheit eines Unternehmens von einem Cyberangriff einschließlich einer Liste mit Indikatoren zur unternehmensinternen Prüfung hinsichtlich eines tatsächlichen Angriffs.

Anwendungsfall 2
Das Unternehmen ist auf dem asiatischen Markt aktiv, plant die Durchführung einer Delegationsreise in die Volksrepublik (VR) China und wünscht hierzu eine Beratung durch das LfV Hamburg.

Anwendungsfall 3
Aus dem Informationsaufkommen (Open-Source-Intelligence-(OSINT-)Recherchen, Austausch mit verschiedenen Unternehmen, Kontakt mit dem BfV) ergeben sich Hinweise auf die mögliche Involvierung eines Unternehmens in Maßnahmen zur Umgehung der Sanktionen gegen die Russische Föderation.

Abwehrmaßnahmen und die Rolle des Verfassungsschutzes:

- Das LfV berät und sensibilisiert Unternehmen und Forschungseinrichtungen und bereitet Erkenntnisse zu möglichen Angreifern, den Zielen und Methoden bedarfsgerecht auf.
- Für das Abhalten von Sensibilisierungsvorträgen wird auf das umfangreiche Präventionsmaterial der „Initiative Wirtschaftsschutz“ zurückgegriffen, welches die Expertise von Staat, Wirtschaft und Wissenschaft bündelt.
- Der VS-Verbund übernimmt hierbei die Rolle eines Frühwarnsystems zur Verhinderung von Spionage- und Sabotageaktivitäten ausländischer Nachrichtendienste in den Bereichen Wirtschaft und Wissenschaft.
- Der VS-Verbund unterstützt Wirtschaftsunternehmen und wissenschaftliche Einrichtungen bei der Detektion und Abwehr von Cyberangriffen.

Sabotageakte

Sabotageakte durch fremde Staaten oder von extremistischer Seite können weitreichende Auswirkungen haben. Das gilt insbesondere mit Blick auf Kritische Infrastrukturen (KRITIS) und KRITIS-nahe Unternehmen.

Beispiele

Brandanschläge auf Infrastruktur der Bahn

Anschlag auf Gaspipelines, Stichwort Nordstream

Ausspähversuche

Ausländische Nachrichtendienste besitzen ein hohes Aufklärungsinteresse zur Gewinnung von vertraulichen Informationen aus Politik, Wirtschaft, Forschung, Wissenschaft und Militär.

Bei vielen autoritären Staaten liegt der Fokus der Nachrichtendienste zusätzlich auf der Ausspähung und Bekämpfung oppositioneller Gruppierungen und Personen im In- und Ausland.

Die Informationsbeschaffung erfolgt hierbei sowohl mit menschlichen Quellen (HUMINT) als auch mit technischen Aufklärungsmaßnahmen (Überwachung der Telekommunikation, Cyberangriffe zur Gewinnung von Datenzugriffen)

Beispiele

Die Nachrichtendienste der VR China nutzen für die Anwerbung von interessanten Zielpersonen beispielsweise Soziale Netzwerke wie LinkedIn.

Die Nachrichtendienste der Russischen Föderation gewinnen ihre Informationen durch die Anwerbung und Führung von Quellen und führen Cyber- und Desinformationskampagnen durch.

Abwehrmaßnahmen und die Rolle des Verfassungsschutzes:

Durch die ständige Weiterentwicklung der technischen Methoden (Einsatz von KI und Quantencomputern) werden Spionageaktivitäten komplexer und lassen sich nur durch einen intensiven Ressourceneinsatz erkennen und verhindern.

Die globale Vernetzung in sämtlichen Themenbereichen (Politik, Wirtschaft, Forschung, Wissenschaft und Militär) nimmt weiter zu und begünstigt Spionageaktivitäten.

Schutz Kritischer Infrastrukturen (KRITIS)

Was KRITIS sind und welche Bedeutung sie haben, wurde bereits in Kapitel 1 Ausgangsüberlegung/Einleitung erläutert (vgl. Abbildung 2: Kritische Infrastrukturen).

Abwehrmaßnahmen und die Rolle des Verfassungsschutzes:

- Permanente Überwachung und Analyse der Spionageaktivitäten fremder Nachrichtendienste durch die Spionageabwehr in Bund und Ländern unter Anwendung nachrichtendienstlicher Mittel
- Sammlung von Hintergrundinformationen zur Arbeitsweise gegnerischer Nachrichtendienste durch operative Verdachtsfallbearbeitungen
- Abgabe von hinreichend bestätigten Verdachtsfällen an die Exekutive zur Einleitung entsprechender Ermittlungsverfahren
- Präventionsmaßnahmen in Wirtschaft, Wissenschaft, Politik und Verwaltung durch Sensibilisierungsvorträge und Einzelgespräche mit relevanten Ansprechpartnern (Vorstände, Sicherheitsbeauftragte, Exportkontrollbeauftragte) zu einzelnen Spionagerisiken in den jeweiligen Bereichen
- Ständiger Austausch mit Sicherheitsverbänden und Wirtschaftsunternehmen zu einzelnen Präventionsthemen (Sicherheit bei Auslandsreisen, Know-how-Schutz und so weiter)
- Erstellung von Sicherheitshinweisen durch den VS-Verbund zur offenen Weitergabe an die Bedarfsträger in Wirtschaft, Wissenschaft und Politik
- Zusammenarbeit mit anderen Sicherheitsbehörden wie Bundesnachrichtendienst (BND), Bundesamt für den Militärischen Abschirmdienstes (BMAD), Bundeskriminalamt (BKA), Zollkriminalamt (ZKA) und so weiter für den Austausch zu aktuellen Entwicklungen im Bereich der Spionageabwehr.

6.3.3 Handlungsnotwendigkeiten

Die Öffentliche Sicherheit ist im vorliegenden Ausgangsszenario nicht ohne nachrichtendienstliche Erkenntnisgewinnung möglich (Lagebild). Deshalb ist eine systematische enge Abstimmung zwischen Nachrichtendiensten, Bundeswehr und Polizei zur Identifikation und Abwehr Hybrider Bedrohungen und Schwachstellen erforderlich.

Die Verfassungsschutzbehörden des Bundes und der Länder, der BND und das BMAD müssen in technischer, personeller und organisatorischer Hinsicht noch besser befähigt werden, die besonderen Herausforderungen in einem militärischen Krisenfall bewältigen zu können.

Der Schutz von KRITIS, insbesondere in den Bereichen Energie, Transport und Kommunikation, erfordert enge Kooperation zwischen Nachrichtendiensten und der Privatwirtschaft.

Die Nachrichtendienste müssen Desinformationskampagnen schnell erkennen und Gegenmaßnahmen vorschlagen, um gesellschaftlichen Spaltungen entgegenzuwirken.

6.3.4 Polizei – Ausgangssituation

„Die Polizeien des Bundes und der Länder sind eine tragende Säule in der Sicherheitsarchitektur in Deutschland. Sie gewährleisten die Bewahrung und Aufrechterhaltung der Inneren Sicherheit. Dabei sehen sie sich […] mit immer komplexeren Herausforderungen in der Einsatzbewältigung konfrontiert."

(Auszug aus dem Eckpunktepapier – Handlungserfordernisse aus polizeilicher Sicht aufgrund strategisch relevanter Lageentwicklungen (VS-NfD), Stand: 12.09.2024 – Bayerisches Staatsministerium des Innern, für Sport und Integration Sachgebiet C5 – Einsatz der Polizei – Geschäftsstelle UA FEK, Odeonsplatz 3, 80539 München)

Auch die Änderungen in der Sicherheitslage in Europa schlagen sich in neuen Herausforderungen nieder. Die Bundeswehr, Garant für die äußere Sicherheit, stimmt deshalb den militärischen Operationsplan für Deutschland (OPLAN DEU) hinsichtlich der Auswirkungen auf die Innere Sicherheit mit den Polizeien des Bundes und der Länder ab. Nachfolgende Herausforderungen sind dabei mindestens zu beachten.

6.3.5 Allgemeine Herausforderung bei der Verlegung von NATO-Truppen – Aufgabe der Polizei

Im Zuge eines Spannungs-, Krisen- oder Verteidigungsfalles werden Truppen der NATO mit der entsprechenden Technik/Logistik an deutsche Außengrenzen verlegt werden müssen. Hierzu bedarf es eines jederzeit aktivierbaren Netzwerkes über alle Verkehrsträger, um ein verzugsloses Transitieren aller NATO-Truppen und deren bruchfreie Versorgung zu gewährleisten. Zu dieser Lageentwicklung und der daraus resultierenden Handlungserfordernisse bedarf es einer aktuellen Bestandsaufnahme. Diese konzentriert sich auf die festgelegten und definierten Schwerpunkte: Grenzübergangspunkt (BCP/Border Crossing Point), Verkehrsträger Schiene, Straße, Häfen und Flughäfen sowie Rastraum (CSC/Convoy Support Center) und Aufmarschraum (MA/Marschalling Area).

Grenzübergangspunkt – Border Crossing Point (BCP)

Es ist beabsichtigt, dass NATO-Truppen BCP verzugslos und mit geringem administrativem Aufwand und unabhängig von einer Tageszeit passieren werden. Hierzu werden neben allgemeinen Grundsatzfragen (wie beispielsweise die Abstimmung zur zivil-militärischen Führung und dem damit einhergehenden, zu steuernden Informationsfluss der Verlegeaktivitäten und –planung) auch die Organisation von Zollabfertigungen und die Bearbeitung von Presseanfragen zählen. Bei den Grenzübergängen muss zwingend berücksichtigt sein, dass innerhalb der EU grundsätzlich offene Grenzen bestehen und grundsätzlich keine Personenkontrolle vorgesehen ist. Durch Zoll und Bundespolizei werden lediglich Sicht- und gegebenenfalls Personenkontrollen von Grenzpendlern und Transportunternehmen durchgeführt. Bei der Verlegung von NATO-Truppen an die entsprechenden Grenzübergangspunkte kann es daher zu unvorhersehbaren Problemen und zu einer Unübersichtlichkeit/Mischung mit dem Personen-/Pendlerverkehr kommen, was nachfolgende Probleme zur Folge haben kann:

- Stau an Grenzübergängen: Vor allem, wenn die Verlegung zu einer ungünstigen Zeit gewährleistet werden muss, können Staus aufgrund von Ferien-/Urlaubszeit, lange Wochenenden oder Großveranstaltungen die Verlegung von NATO-Truppen beeinflussen. Weiter erschwerend könnten zusätzliche Ereignisse wie eine Tierseuchenprophylaxe (etwa bei Afrikanischer Schweinepest, Vogelgrippe oder ähnlichem) oder Naturereignisse (beispielsweise Hochwasser) wirken, die die Grenzabwicklung erschweren/verzögern.

- Spontan-Demonstrationen: So könnten Friedensaktivisten Truppenverlegungen verhindern wollen und Grenzübergänge blockieren. Ergänzend könnten weitere Demonstrationen hinzutreten, um Forderungen mehr Nachdruck zu verleihen (vergleiche die Bauernblockaden 2024 der Bundesautobahnen).

- Cyberangriff auf IT-Infrastrukturen, die den Grenzübergang unterstützen.

- Flüchtende: Die Unübersichtlichkeit an den Grenzen kann dazu führen, dass die Organisierte Kriminalität, zum Beispiel auch im Bereich Schleusung, stark zunimmt.

- „Falsche Flüchtende“: Die Unübersichtlichkeit könnte auch bewusst zur Einschleusung von Verfassungsfeinden in die Bundesrepublik Deutschland ausgenutzt werden.

Verkehrsträger Straße

Die Truppen müssen das öffentliche Straßennetz (vorzugsweise Autobahnen aufgrund ihrer Fahrbahnbreiten und Gewichtsklassen), unabhängig von der Tageszeit und dies mit möglichst geringen Auswirkungen auf die Zivilbevölkerung nutzen können. Neben den Grundsatzfragen im Hinblick auf zivil-militärische Führungsorganisation, Informationssteuerung an Behörden/Institutionen, Presse und Bevölkerung, Implementierung von standardisierten, vereinfachten Verfahren – beispielsweise Schwerlasttransport (SLT) – sowie die Trennung des Militärstraßengrundnetzes (MSGN) und des Hauptzivilstraßengrundnetzes (HZGN) sind folgende Herausforderungen zu berücksichtigen:

- Mögliche Brücken- oder Tunnelsperrungen auf den Autobahnen (vgl. etwa die Sperrungen der Rheinbrücke bei Leverkusen, Rader Hochbrücke über den Nord-Ostsee-Kanal oder die Absackung der A 20 bei Tribsees); dies könnte zu einer überplanmäßigen Nutzung einer Ausweichroute/HZGN mit den NATO-Truppen einschließlich SLT führen. Die Infrastruktur der Ausweichroute könnte für den SLT nicht geeignet sein.

- Sabotagehandlungen an Straßeninfrastrukturen

- Staus auf den Autobahnen aufgrund von Urlaubs-/Ferienzeit bzw. als „faktische Demonstrationen“ zur Erschwerung der Nutzbarkeit

- Ereignisse wie Unfälle (gegebenenfalls mit Gefahrgutbeteiligung) oder Witterungseinwirkungen (wie Schnee, Eis, Regen oder Sandsturm)

- Streik des Straßenunterhaltungspersonals

Verkehrsträger Schiene

Insbesondere auch Gerätschaften und Fahrzeuge könnten deshalb auf dem Verkehrsträger Schiene transportiert werden. Neben den auch hier einschlägigen Grundsatzfragen der zivil-militärische Führungsorganisation (Melde- und Entscheidungswege) und der Trennung des MSGN von dem zivilen Netz können auch hier Probleme auftreten wie:

- Cyberangriffe/Sabotage auf Bahnanlagen (Stellwerke, Weichen, Verladeeinrichtungen)

- Angriffe auf die Bahnkommunikation

- Vorliegen von Schienenersatzverkehr (Bahnstrecken könnten aufgrund von Bauarbeiten nicht zur Verfügung stehen; vgl. die Streckensperrung Berlin-Hamburg)

- Ungeplante Ereignisse wie Witterungsverhältnisse beeinträchtigen die Nutzbarkeit der Bahnanlagen

- Demonstration oder Blockaden auf den Bahnstrecken/Bahnübergängen (vergleiche Gorleben-Blockaden)

- Streik des Bahnpersonals.

Verkehrsträger Hafen – Seaport of Debarkation (SPOD) und Flughäfen

SPODs und Flughäfen dienen zur Be- und Entladung von Roll-on-roll-off-Schiffen oder Frachtflugzeugen. Dazu ist ein Aufmarschraum (MA) im selben Raum zu belegen und dient dem Abstellen und Auffahren von Fahrzeugen sowie zum Zwischenlagern von Containern. Verkehrsträger wie Straße und Schiene sollten ebenfalls in unmittelbarer Reichweite liegen. Da die meis-

ten SPOD und Flughäfen zivil betrieben werden, ergeben sich auch hier die Grundsatzfragen der zivil-militärischen Führungsorganisation (Melde- und Entscheidungswege), dies allerdings mit privatwirtschaftlich Handelnden. Ferner ist hier die Nutzbarkeit besonders zu regeln, da diese – anders als beim Verkehrsträger Straße – vertraglich an die Nutzenden vergeben sind. Nachfolgende Probleme könnten in diesem Bereich in Erscheinung treten:

- Sicherung der Infrastruktur
- Vertragliche Bindungen der Kapazitäten (zum Beispiel für die Nahrungsmitteltransporte)
- Demonstration, Blockaden (vergleiche „Letzte Generation“)
- Organisierte Kriminalität: Höheres Kriminalitätsaufkommen (eskalierende Demonstrationen, Sabotage, Schleusung von Personen und so weiter)
- Cyberangriff auf IT-Infrastrukturen oder Betriebssysteme (siehe Störungen des Global Positioning Systems GPS) blockieren die Infrastrukturen
- Maritime Notlagen (Beteiligung des Havarie-Kommandos)
- (Unterwasser-)Drohnen
- Streik des Hafen-/Flughafenpersonals

Rastraum – Convoy Support Center (CSC)

Unter dem Begriff Rastraum wird ein Ort in räumlicher Nähe zu den Verlegekorridoren für die „Regeneration“ marschierender militärischer und ziviler Kräfte (NATO) durch Fahrtunterbrechung verstanden. Auch hier ergeben sich Grundsatzfragen, wie die Sicherstellung des Schutzes des entsprechenden Objektes/Geländes oder die Übernahme der zivil-militärische Führungsorganisation (Melde- und Entscheidungswege). Versorgungs- und Gesundheitssicherstellung der Truppen muss gewährleistet werden, was eine Verzahnung mit zivilen und militärischen Institutionen darstellt. Hier könnten Probleme entstehen wie:

- Demonstrationen/Blockaden an den Autobahnauf- und -abfahrten
- Demonstrationen/Blockaden an den Zu- und Abfahrten des CSC
- Erhöhtes Kriminalitätsaufkommen im Zusammenhang mit dem CSC (Sabotage, Kleinkriminalität und so weiter)
- Beeinträchtigungen der Grundversorgung durch Strom- und Wasserversorgung durch Sabotage oder einer Störung der Versorger. Die Versorgung des CSC selbst (Essensversorgung und Ähnliches) könnte wiederum erschwert sein, wenn der Vertragspartner aufgrund einer Autobahnsperrung/Blockaden auf der Lieferstrecke behindert ist.
- Beeinträchtigung der Treibstoffversorgung und anderer Betriebsgüter des CSC
- Sicherung des CSC-Rastraums beispielsweise vor Drohnenüberflügen oder vor möglichen Beschädigungen der Infrastruktur des Rastraumes
- Ungeplante Ereignisse wie Witterungsverhältnisse könnten die Nutzbarkeit des CSC beeinträchtigen.

Marschalling Area (MA)/Aufmarschraum

Eine MA gilt als Zusammenführungs-/Umschlagsort von Fahrzeugen und Personal. In der MA werden die entladenen Fahrzeuge von der Drivers Party (DP) den Kommandanten und Kraftfahrern (MKF) des Fahrzeugs (Vehicle Party) übergeben. Dabei kann die Vehicle Party für eine begrenzte Zeit in der MA verbleiben. Der MA ist deshalb oftmals in der Nähe von Verkehrsträgern. Gegebenenfalls müssten hier noch spezielle Baumaßnahmen zuvor genehmigt werden (Melde- und Entscheidungswege). Auch für MA ergeben sich Problemlagen wie:

- Demonstrationen könnten vor dem Gelände der MA oder den in der Nähe befindlichen Autobahnab- und -auffahrten sowie den Hafenein- und -ausfahrten oder dem Schienennetz (Railhead) durchgeführt werden.

- Ausfall von Strom- und Wasserversorgung, Vertragspartner kann Verpflegung erst verspätet bereitstellen

- Drohnensichtung und höheres Kriminalitätsaufkommen durch eskalierende Demonstrationen, Sabotage und so weiter

- Ungeplante Elemente wie Witterungsverhältnisse, Unfälle und Ähnliches

- Desinformationskampagne

- Verzögerung der Drivers Party

6.3.6 Polizeimaßnahmen und resultierende Handlungsnotwendigkeiten

Die Truppentransporte, verbunden mit dem einhergehenden Logistikaufwand, werden dazu führen, dass das zivile Leben stark beeinflusst werden wird. Daraus ergeben sich Einschränkungen/Beschränkungen für den Öffentlichen Verkehr und die Mobilität der Bevölkerung. Dies kann auch dazu führen, dass die Versorgung nur eingeschränkt oder verzögert aufrechterhalten werden kann. Das führt dazu, dass ganz gesteigerte Anforderungen an die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung im Land zu stellen sind. Die „Unruhen“ könnten forciert und angestachelt werden, um zu einem Zustand allgemeiner Unruhe zu gelangen (politische Destabilisierung). Auch Organisierte Kriminalität sowie die sonstige Kriminalität könnten sich diesen Zustand zunutze machen. Folgende polizeiliche Maßnahmen und damit einhergehende Handlungsempfehlungen ergeben aus diesen Problemfeldern:

1. Aufrechterhaltung der Inneren Sicherheit durch erhöhte Polizeipräsenz

- Sichtbare Polizeipräsenz dient der Prävention und müsste so für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sorgen. Einsatzeinheiten müssen dazu flexibel und schnell handlungsfähig sein. Dies muss in Ballungszentren und an strategisch wichtigen Orten wie Flughäfen, Wasserhäfen, Bahnhöfen, Verkehrsknotenpunkten, Regierungsgebäuden, Versorgungsträgern und Grenzübergangspunkten berücksichtigt werden.

- Schutz Kritischer Infrastrukturen (KRITIS): Wichtige Infrastrukturen wie Strom- und Wasserversorgung, Kommunikationsnetze und Transportwege müssten durch Objektschutzmaßnahmen besonders geschützt werden, um die Funktionsfähigkeit der Gesellschaft weiter gewährleisten zu können.

- Schutz der Staats- und Regierungsfunktionen

- Schutz von Versammlungs- und Demonstrationslagen: Die sicherheitspolitische Lage (Truppenbewegung) und die sich daraus ergebenden Folgen werden zu einer Steigerung des Versammlungs- und Demonstrationsgeschehens führen, das durch die Polizeien zu schützen ist und daher deren Einsatzkräfte bindet.

- Ferner ist von einem steigenden Kriminalitätsaufkommen auszugehen (teils aus einer Not heraus, massiv aber auch durch Ausnutzung der besonderen Lage).

Daraus resultierende Handlungsnotwendigkeiten:

- Stärkung der Polizeistrukturen durch Einrichtung von zusätzlichen geschlossenen Einheiten vorzugsweise in den Bereitschaftspolizeien. Die Einheiten müssen organisatorisch flexibel dort unterstellt werden können, wo sie benötigt werden.

- Die wichtige Rolle des Inspekteurs der Bereitschaftspolizeien im BMI insbesondere als

Koordinator für die notwendige Zusammenarbeit zwischen Bund und Ländern ist zu verstetigen.

- Stärkung auf materieller und taktischer Ebene durch moderne, krisenfeste Mann-Ausstattung und entsprechender einsatztaktischer Trainingseinheiten zusammen mit Bundespolizei und Bundeswehr.

- Das „Trennungsgebot“ im Informationsaustausch zwischen dem Verfassungsschutz und der Polizei muss für Krisen- und Verteidigungsfälle so ausgestaltet sein, dass es zu keiner (Informations-)Einbuße in der Öffentlichen Sicherheit führen kann.

- Mindset in der Polizei: Der Polizeidienst muss in solchen Szenarien klar definiert und beübt worden sein.

- Zurverfügungstellung und Nutzung innovativer Technologien/Künstliche Intelligenz (KI)

2. Zusammenarbeit Polizei und Streitkräften

- Kommunikation und Transparenz: Sowohl für die Streitkräfte als auch für die Polizei muss ein vollumfängliches und einheitliches Lagebild geschaffen werden, welches durch einen ständigen Austausch aktuell gehalten wird. Das Lagebild muss einen aktuellen Aufschluss über die zuvor benannten Problemfelder als auch über Verlegepläne und gebundene Einsatzkräfte in polizeilichen Maßnahmen geben. Hier muss der Fokus auf eine einheitliche Kommunikation mit festgelegten und geübten Strukturen liegen.

- Koordination von Ressourcen: Enge Zusammenarbeit und Koordination mit der Bundeswehr sind notwendig, insbesondere, wenn diese zur Unterstützung der Inneren Sicherheit eingesetzt oder die Polizei für die Absicherung der Transportstrecken von NATO-Truppen benötigt werden.

- Abstimmung von Maßnahmen: Die Festlegungen des OPLAN DEU müssen in der Polizei abgestimmt und entwickelt werden, um Überschneidungen und ineffiziente Doppelstrukturen zu vermeiden.

- Status der Polizei (Kombattantenstatus) muss geklärt sein.

Daraus resultierende Handlungsnotwendigkeiten:

- Klare Festlegung/Abgrenzung von Zuständigkeiten der Polizei und Bundeswehr, beispielsweise im Hinblick auf die Begleitung von NATO-Truppen und Logistiktransporten gegebenenfalls durch Verkehrslenkungen/Sperrungen von Autobahnen oder auch die Begleitung/Sicherung von Demonstrationen

- Befähigung der Streitkräfte zur eigenen Anmeldung/Genehmigung/Begleitung von militärischen Schwerlasttransporten

- Schaffung von Befugnissen für Militärpolizei-Feldjäger zur Verkehrsregelung (auch in „Friedenszeiten“)

- Schaffung niederschwelliger ordnungspolizeilicher Befugnisse für Militärpolizei-Feldjäger, wie etwa Aussprechen von Platzverweisen, Datenabfragen bei Behörden

- Festlegung der Befugnisse des Heimatschutzes der Bundeswehr/Abgrenzung zur Polizei

- Festlegung und Abstimmung von zu schützenden Objekten mit kritischen zivil- oder militärischen Infrastrukturen sowie der Koordinierung der Schutzmaßnahmen mit den Streitkräften unter Beteiligung von privaten Sicherheitsfirmen.

3. Kontrolle und Überwachung der Grenzen

- Verstärkte Grenzkontrollen und -überwachung: Sollte es zu einem erhöhten Sicherheitsrisiko durch Flüchtlingsströme, Sabotageaktionen, Hybride Bedrohungen, Organisierter Kriminalität oder den Aufmarsch von feindlichen Kräften an den Grenzübergängen kom-

men, müsste die Bundespolizei gegebenenfalls verstärkte Grenzkontrollen durchführen.

- Unterstützung der Bundespolizei: Um illegale Grenzübertritte einzudämmen und die damit einhergehende nationale Sicherheit zu gewährleisten, müsste die Landespolizei gegebenenfalls. die Bundespolizei bei der Realisierung ihrer Aufgaben unterstützen. Auch hier muss geprüft werden, ob die Militärpolizei-Feldjäger der Bundeswehr oder bereits eingesetzt NATO-Truppen bei dem Grenzschutz eingebunden werden können.

- Nutzung innovativer Technik wie moderne Überwachungstechnik oder KI

Daraus resultierende Handlungsnotwendigkeiten:

- Vereinfachung der Verfahren beim Grenzübertritt von NATO-Streitkräften

- Personalaufstockung von Zoll und Bundespolizei

- Prüfung von Aufgaben, die gegebenenfalls durch zivile Unternehmen oder durch die Bundeswehr übernommen werden können.

4. Umsetzung von Notfall- und Krisenplänen

- Feststellung Spannungs-/Bündnis-/Verteidigungsfall: Feststellung der Auswirkungen der Sicherstellungs- und Vorsorgegesetze auf die Arbeit und die Befugnisse der Polizei.

- Maßnahmengesetze: Prüfung des Bedarfs, ob im Rahmen eines Krisen- oder Verteidigungszustands Maßnahmengesetze aktiviert werden müssen, die den Polizeien erweiterte Befugnisse zugestehen.

- Evakuierungs- und Katastrophenmanagement: Prüfung der Beteiligung der Polizeien im Rahmen von Evakuierungen, des Einrichtens und des Unterhaltens von Notunterkünften zur Unterstützung der beauftragten Hilfsorganisationen.

- Warnung der Bevölkerung/Informationsmanagement: Regelmäßige Kommunikation und klare Anweisungen an die Bevölkerung sind entscheidend, um Vertrauen zu erhalten beziehungsweise zu schaffen. Die Polizeien sollten deshalb in die Kommunikation mit der Bevölkerung mit eingebunden werden.

Daraus resultierende Handlungsnotwendigkeiten:

- Strukturierung der Prozesse und Aufgaben der Beteiligten (Bundeswehr, Feuerwehren, Katastrophenschutzeinheiten, Technisches Hilfswerk (THW), Polizeien und weiteren Hilfsorganisationen)

- Nutzung innovativer Technik wie KI oder anderer Plattformen für die Warnung/Aufklärung der Bevölkerung

5. Zivilschutz und Zivile Verteidigung

- Präventivmaßnahmen: Abstimmung eines Kanons von Präventivmaßnahmen der Ordnungsbehörden/Polizeien im Falle von Krisen- oder Verteidigungsfällen

- Aufklärung und Beratung der Bevölkerung durch Polizei, Feuerwehren, Katastrophenschutzeinheiten, THW und weiteren Hilfsorganisationen über Schutzmaßnahmen, Verhaltensregeln und Evakuierungspläne

- Strukturierung der Zusammenarbeit und des Informationsaustausches zwischen den Behörden und internationalen Partnern (EU und NATO)

- Nachrichtendienste: Die Zusammenarbeit mit den Nachrichtendiensten muss so gestaltet sein, dass Bedrohungen für die öffentliche Sicherheit erkannt und unterbunden werden können.

- Verstärkte Einbeziehung ziviler Firmen in die Sicherheitsarchitektur.

Daraus resultierende Handlungsnotwendigkeiten:

- Bereits im Vorfeld müssen Positionen (ZMZ-Beauftrage) in Ministerien, Behörden und Institutionen geschaffen werden, die intern und extern Ansprechperson sind.
- Rechtliche Grundlagen/Befugnisse für präventive Maßnahmen müssen vorbereitet vorliegen.
- Das Zusammenwirken von Behörden und Hilfsorganisationen in einem Krisen- oder Verteidigungsfall muss durch klare Aufgaben und Strukturen gewährleistet werden. Hierzu müssen entsprechende Übungen und Workshops organisiert und durchgeführt werden, aus denen weitere Handlungsnotwendigkeiten entwickelt werden.

6.3.7 Rolle und Aufgaben des Brand- und Katastrophenschutzes, Rettungsdienste

Die öffentliche Sicherheit und Ordnung wird ganz wesentlich auch durch die Bereiche „Brandschutz“, „Rettungsdienst“ und „Katastrophenschutz“ als zivile Bereiche der staatlichen Daseinsvorsorge geleistet und durch diese geprägt. Die Zahl der hier tätigen Einsatzkräfte übersteigt die Zahl der Einsatzkräfte in den Bereichen „Polizei“ und „Verfassungsschutz“ deutlich.

Diese Zivilschutzorganisationen sind eng in die Weiterentwicklung der ZMZ 4.0 auf allen Ebenen einzubinden. Nur so kann der Nutzen dieser Organisationen seine Wirkung entfalten.

6.4 Zivil-Militärische Zusammenarbeit bei Bedrohungen der Kritischen Infrastrukturen

Die Zivile Verteidigung als Teil der Gesamtverteidigung gliedert sich in vier Handlungsfelder: Die Aufrechterhaltung der Staats- und Regierungsfunktionen, den Zivilschutz, die Versorgung der Bevölkerung und die Unterstützung der Streitkräfte.

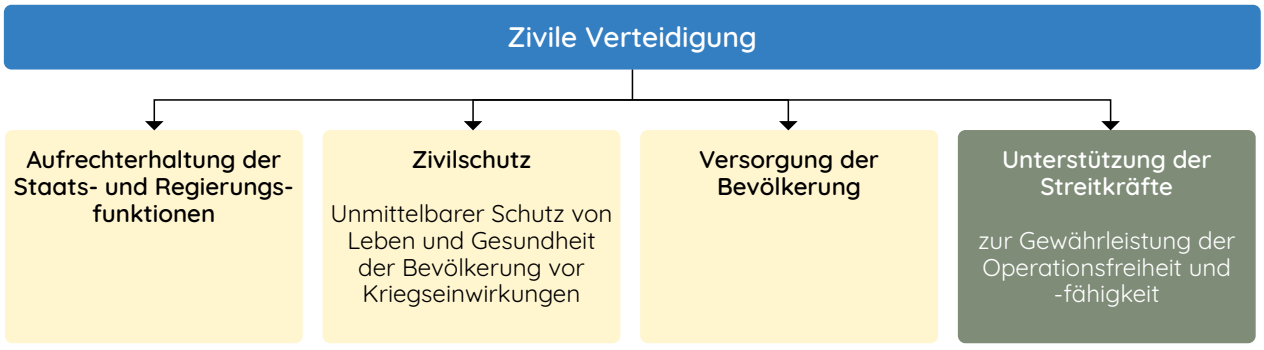

Abbildung 10: Zivile Verteidigung

Die Wirtschaft und die Verwaltung unseres Landes müssen hinreichend leistungsfähig und resilient sein, um dies zu unterstützen und die Grundversorgung staatlicher und privatwirtschaftlicher Akteure sowie der gesamten Bevölkerung auch unter schwierigen Bedingungen sicherzustellen.

In Zeiten Hybrider Bedrohungen wie sie im Ausgangsszenar 2030 beschrieben sind, ist diese Grundversorgung nicht nur durch kriminelles Handeln, sondern auch durch Aktivitäten von Extremisten, Terroristen und verdeckt operierenden militärischen Spezialeinheiten bedroht.

Die Kritischen Infrastrukturen (KRITIS) in Wirtschaft und Verwaltung stellen für die (potenziellen) Angreifer aufgrund ihrer Relevanz für die Gesamtverteidigung besonders lohnende Ziele dar.

Im Wirtschaftsschutz 2024+, der sich als Gemeinschaftsleistung staatlicher und privatwirtschaftlicher Akteure auf die Stärkung der Resilienz der Wertschöpfungs- und Lieferketten ausrichtet, erhält der Schutz der KRITIS daher eine besondere Bedeutung.

Die Unterstützung, die unsere Streitkräfte zur Gewährleistung der Operationsfreiheit und -fähigkeit im Rahmen der Zivil-Militärischen Zusammenarbeit (ZMZ) erhalten, wird somit auch von der Resilienz der KRITIS abhängen.

> *Die Betreiber der KRITIS müssen die verfügbaren Technologien zum Schutz der Anlagen nutzen, damit unsere Kritischen Infrastrukturen bestmöglich vor Angriffen und Sabotage gesichert werden.*
>
> *Bund, Länder und Kommunen müssen die Zuständigkeiten und Verfahren der Zusammenarbeit klären, um Schäden gut bewältigen zu können.*
>
> *– Ingo Schäfer MdB*

6.4.1 Schutzziele beim Schutz Kritischer Infrastrukturen

Schutzziele für KRITIS machen Aussagen darüber, was durch deren Schutz erreicht werden soll. Beispielhafte Schutzziele für Kritische Infrastrukturen können sein:

1. Das frühzeitige Erkennen von geplanten Angriffen auf Kritische Infrastrukturen
2. Das Erschweren von Angriffen auf Kritische Infrastrukturen
3. Die frühzeitige Alarmierung bei Angriffen auf Kritische Infrastrukturen
4. Das Verifizieren von Angriffen nach erfolgter Alarmierung
5. Das Eintreffen professioneller Interventionskräfte gemäß vereinbarter Reaktionszeit
6. Die Begrenzung des Schadensausmaßes von Angriffen nach dem Eintreffen von Interventionskräften
7. Die rasche Einleitung und gegebenenfalls überregionale Koordinierung von Sofortmaßnahmen
8. Die weitgehende Aufrechterhaltung des Betriebs beziehungsweise der geplanten Geschäftsaktivitäten
9. Die rasche Instandsetzung der eingetretenen Schäden
10. Die rasche Wiederherstellung des Normalzustandes

Inwieweit diese Schutzziele erreicht werden können, hängt insbesondere von der „Schützbarkeit“ der jeweiligen Infrastruktur, von der Intensität der Bedrohung, bzw. davon, welche Tätergruppe bzw. Täterkategorie die Infrastruktur angreift und von dem „Sicherheitsbudget“, mit dem die jeweiligen baulichen, technischen, organisatorischen und personellen Schutz- und Resilienz-Maßnahmen finanziert werden, ab.

6.4.2 Die „Schützbarkeit“ von Kritischen Infrastrukturen

In Bezug auf ihre „Schützbarkeit“ lassen sich Kritische Infrastrukturen in folgende Kategorien einteilen:

Kategorie A:
Abgegrenzte, umschlossene und umschließbare Infrastrukturen auf einem (eigenen) Grundstück, bei denen das Schutzprinzip „Ritterburg“ beziehungsweise eine Rundumsicherung möglich ist.

Kategorie A 1:
In oder in der Nähe von Siedlungen und Polizeipräsenz; eine rasche Erreichbarkeit durch Interventionskräfte ist im Alarmierungsfall möglich (Beispiel: Rechenzentrum in einer Großstadt).

Kategorie A 2:
Abgelegen in Wald und Feld abseits von Siedlungen und Polizeipräsenz; eine rasche Erreichbarkeit durch Interventionskräfte ist im Alarmierungsfall nicht oder nur unzureichend möglich (Beispiel: Umspannwerk in einem Wald auf der Schwäbischen Alb).

Kategorie B:
Nicht oder nur schwer abgrenzbare und nicht oder kaum umschließbare Infrastrukturen, die sich quer durch das Land ziehen (Beispiele: Brücken, Schienen, Gasleitungen, Hochspannungsleitungen), bei denen das Schutzprinzip „Ritterburg“ beziehungsweise eine Rundumsicherung nicht möglich und auch eine rasche Erreichbarkeit durch Interventionskräfte häufig nicht gegeben ist.

6.4.3 Täterkategorien und die Intensität der Bedrohung

Für die Beschreibung der Sicherheitslage an einer Kritischen Infrastruktur bzw. wie „gefährlich“ die (aktuelle) Situation für eine Kritische Infrastruktur ist, gibt es verschiedene Ansätze.

Orientiert man sich hierbei vorrangig an den potenziellen Tätern, so können diese in verschiedene Täterkategorien sortiert beziehungsweise eingeordnet werden.

In Anlehnung an die „**in Friedenszeiten**“ entstandene Normen wie die DIN EN 1627 (Einbruchshemmung) lassen sich folgende drei Tätertypen beziehungsweise Täterkategorien beschreiben

- Gelegenheitstäter („Anfänger“)
- Gewohnt vorgehender Täter („Fortgeschrittener“)
- Erfahrener Täter („Profi“)

Die Kategorie „extremistische und terroristische Einzeltäter und Gruppen“ ist in diesen Normen nicht vorgesehen, wohl aber in einer „Gefährdungsartentabelle“ des Bundesministeriums des Innern und für Heimat (BMI). Dort ist diese Täterkategorie in der „Gefährdungsart 3“ zugeordnet (BMI 2005 – Schutz Kritischer Infrastrukturen – Basisschutzkonzept. S. 27).

In Zeiten **Hybrider Bedrohungen** sowie im **Spannungsfall** ist durchaus – zusätzlich – mit Angriffen durch Extremisten und Terroristen zu rechnen.

Außerdem mit Einsätzen von irregulären Kräften, zum Beispiel in Form von militärischen Spezialeinheiten, die sich „undercover“ beziehungsweise als Zivilsten getarnt im Land aufhalten und unter Einsatz hochmoderner Technik sowie militärischen Waffen und Sprengmitteln gut organisierte „Kommando-Operationen“ durchführen.

Im **Verteidigungsfall** muss zusätzlich davon ausgegangen werden, dass auch reguläre gegnerische Land-, Luft- und Seestreitkräfte in hoher Anzahl und mit allen verfügbaren militärischen Aufklärungs- und Wirkmitteln für eine hohe Bedrohungsintensität sorgen.

Die **Bedrohungsintensität** für Kritische Infrastrukturen steigt mit der Leistungsfähigkeit und

Entschlossenheit der Angreifer. Wie oben dargestellt ist die Bandbreite hierbei hoch. In den im Ausgangsszenar 2030 umrissenen Zeiten Hybrider Bedrohungen reicht sie von Beschaffungskriminalität durch „Anfänger“ bis hin zu Sabotageaktionen, die von verdeckt operierenden Spezialeinheiten im Handstreich durchgeführt werden.

Die traditionellen oder für Friedenszeiten entwickelten und in Friedenszeiten bewährten Systematiken und Schutzkonzepte, die im Wesentlichen auf die Abwehr von kriminellem Verhalten ausgerichtet sind, greifen offensichtlich bei den hohen Bedrohungsintensitäten nicht mehr, wie sie im Ausgangsszenar 2030 beispielsweise bei Sabotageaktionen von Terroristen und militärischen Spezialeinheiten zu erwarten sind.

6.4.4 Die Ausprägung der eigenen Fähigkeiten – Schutz und Resilienz

Bei der Beschreibung der Fähigkeiten, die für den Schutz und für die Aufrechterhaltung – oder Wiederherstellung – des Betriebs beziehungsweise der Geschäftstätigkeit von Kritischen Infrastrukturen relevant sind, kann folgende Gliederung genutzt werden:

Prävention

Ein Angriff auf KRITIS wird durch bauliche, technische, organisatorische und personelle Sicherheitsmaßnahmen erschwert.

- Baulich: Zum Beispiel Umfriedung (Zaun; Höhensprünge), Mauerwerk, Fassadenelemente
- Technisch: Zum Beispiel Zutrittssteuerung, bewegliche Sperrelemente, Vereinzelungsanlagen
- Organisatorisch: Zum Beispiel Zonenkonzept, Identity- and Access Management, SOH
- Personell: Zum Beispiel Besuchermanagement, Bestreifung, Schulung von Beschäftigten

Detektion

Ein Angriff auf KRITIS wird erkannt zum Beispiel durch das Auslösen eines Sensors, und dann verifiziert etwa nach Aktivierung einer ereignisgesteuerten Videoaufschaltung durch einen Operator in der Sicherheitszentrale oder durch einen Streifengänger, der sich vor Ort einen Überblick verschafft.

Intervention

Nach der Verifizierung des Angriffs erfolgt eine Alarmierung professioneller Interventionskräfte, die innerhalb der vereinbarten Reaktionszeit (unter anderem abgestimmt auf die Widerstandszeiten der baulichen Infrastrukturen und Fassadenelemente) am Ort des Angriffs eintreffen und den Angriff beziehungsweise die Straftat beenden, bevor sie von den Tätern vollendet werden kann.

Stabilisierung

Parallel zur Ermittlung des Schadensausmaßes beginnen Notfall- und Krisenbewältigung durch Sofortmaßnahmen sowie die Einleitung des Notbetriebs beispielsweise durch Aktivierung von Redundanzen und Einsatz von Reserven. Nach der erforderlichen Instandsetzung und hinreichender Wiederherstellung des Ausgangszustands ist die Rückkehr in den Normalbetrieb möglich.

Alle vier Fähigkeitskategorien sind in einer Mindestausprägung erforderlich, das heißt jede KRITIS benötigt einen angemessenen „Grundschutz“ vor Angriffen in der physischen und der digitalen Welt. Insbesondere dort, wo der Dreiklang von Prävention, Detektion und Intervention nicht (mehr) gelingt, muss durch geeignete Business-Continuity-Management-Planung (BCM-Planung) gewährleistet werden, dass trotz des Ausfalls der angegriffenen Einrichtung oder Anlage die von ihr zu erbringende (Dienst-)Leistung weiterhin verfügbar bleibt (Stabilisierung).

6.4.5 Beispielhafte KRITIS-Anwendungsfälle

Als Grundlage für die Ableitung von Handlungsnotwendigkeiten für eine Verbesserung von Schutz und Resilienz der KRITIS wurden auf Grundlage des Ausgangszenars 2030 drei KRITIS-Szenarien entwickelt.

Der **erste Anwendungsfall** adressiert den Sektor **„Energie“**:

Er beschreibt den Angriff auf ein Umspannwerk im Wald (Kritische Infrastruktur – Kategorie A2) durch eine aus dem Ausland gesteuerte, radikale politische Gruppe mit Sabotage-Erfahrung. Die Gruppe hat sich in den Sozialen Medien zu einer weiteren Straftat verabredet und diese planmäßig durchgeführt.

Der sich entlegen in einem Waldstück befindende Standort des Umspannwerks wurde als Anschlagsziel ausgewählt, weil er von den Interventionskräften erst nach einer recht langen Anfahrt erreicht werden kann. Somit funktioniert der in der Standortsicherheit etablierte Dreiklang von Prävention, Detektion und Intervention dort nicht.

Dementsprechend konnten die Angreifer in das Umspannwerk ohne Eile eindringen, die geschäftskritischen Anlagen und Einrichtungen in aller Ruhe zerstören, ihre Tat vollenden und wieder verschwinden, bevor die Interventionskräfte vor Ort eintrafen.

Ein unzureichendes BCM-Konzept sorgte dafür, dass die Täter ihre Ziele erreichen konnten.

Die Ausprägung der eigenen Fähigkeiten

Fähigkeits-kategorien Schutz und Resilienz	Derzeit vorhanden	Ausgewählte künftig anzustrebende Erweiterungen/Ergänzungen
Prävention	Standortsicherheitskonzept u. a. mit Sicherheitszaun, Zutrittssteuerung, Einbruchmeldeanlage, Widerstandsertüchtigung von Fassadenelementen nach RC4 (Widerstandszeit: je 10 Min.)	OSINT-Aufklärung; „Digital Listening“ Plattform zur Bedrohungsfrüherkennung; Interdisziplinäres Lagebild in Echtzeit
Detektion	Zaunsensoren, Bewegungssensoren, Videokameras, Alarmempfangsstelle	Ggf. Bewachung/Bestreifung vor Ort; Ggf. Einsatz von Aufklärungsdrohnen
Intervention	Eintreffen privater Sicherheitskräfte nach 30 Minuten; Eintreffen der Polizei nach 45 Minuten	Interdisziplinäres Lagebild in Echtzeit; Ggf. Einsatz von Hubschraubern; Ggf. Bewachung/Bestreifung vor Ort
Stabilisierung	Kein „hilfreiches“ Business-Continuity -Konzept	Leistungsfähiges Business Continuity-Konzept mit Redundanz-Planung, Ersatzteil-Bevorratung, Ressourcen zur Schnellinstandsetzung etc. Ggf. unternehmensübergreifendes „Pooling & Sharing“-Konzept; Ggf. Standardisierung von Transformatoren und technischen Bauteilen

Der **zweite Anwendungsfall** adressiert den Sektor **„Informationstechnik“**:

Hier wird ein Rechenzentrum in einer Großstadt (Kritische Infrastruktur – Kategorie A1) durch eine gut ausgebildete Terrorgruppe mit Sprengmitteln und Schusswaffen angegriffen und weitgehend zerstört.

Die aufwändigen und teuren, durchgängig nach RC6/P8B widerstandsertüchtigten physischen Sicherheitsmaßnahmen konnten von diesen Angreifern in Sekunden überwunden werden.

Die Polizeikräfte waren schneller vor Ort, als dies gemäß der Vereinbarung mit dem Standortverantwortlichen zu erwarten gewesen wäre. Dennoch hatten sie die Angreifer nicht mehr angetroffen, da diese bereits nach zehn Minuten ihre Tat vollendet hatten und verschwunden waren. Das BCM-Konzept sah vor, dass bei einem entsprechenden Ereignis unmittelbar nach Alarmierung die Datenverarbeitung für sämtliche Business Operations auf das redundante Notfallrechenzentrum verlagert werden sollen.

Aufgrund des erfolgreich umgesetzten Notfallplans (als Teil der Resilienz-Strategie des Unternehmens) konnten die Angreifer trotz der Zerstörung dieses Rechenzentrums ihr eigentliches Ziel somit nicht erreichen.

Die Ausprägung der eigenen Fähigkeiten

Fähigkeitskategorien Schutz und Resilienz	**Derzeit vorhanden**	**Ausgewählte künftig anzustrebende Erweiterungen/Ergänzungen**
Prävention	Standortsicherheitskonzept u.a. mit Sicherheitszaun, Zutrittssteuerung, Einbruchmeldeanlage, Widerstandsertüchtigung von Fassadenelementen nach RC6 (Widerstandszeit: je 20 Min.)	OSINT-Aufklärung; „Digital Listening“; Plattform zur Bedrohungsfrüherkennung; Interdisziplinäres Lagebild in Echtzeit Versenkbare Sperrelemente am Haupttor; Digitaler Zwilling;
Detektion	Zaunsensoren, Bewegungssensoren, Videokameras, AES, NSL, Bewachung und Bestreifung durch Sicherheitspersonal vor Ort	
Intervention	Rasches Eintreffen der Polizei bereits nach 15 Min. (!)	Interdisziplinäres Lagebild in Echtzeit
Stabilisierung	Durchdachtes BCM- Konzept – unter anderem rasche Verlagerung der Business Operations auf ein redundantes Notfallrechenzentrum	

Der **dritte Anwendungsfall** adressiert den Sektor **„Transport und Verkehr“**:

Durch einen angenommenen Unfall wird eine Eisenbahnbrücke über eine Wasserstraße (Kritische Infrastruktur – Kategorie B) zerstört, nachdem ein Schiff mit einem Brückenpfeiler kollidiert ist. Durch einen glücklichen Umstand kann diese kurzfristig instandgesetzt und wieder in Betrieb genommen werden. Kurze Zeit später zerstört ein zweiter, ähnlicher Unfall die Brücke jedoch vollständig.

Die Brücke ist eine überregional wichtige Infrastruktur, die vor allem auch für die militärische Logistik benötigt wird. Untersuchungen ergeben, dass hier zweimal hintereinander eine Sabotageaktion aus dem Bereich elektronische Kampfführung (EloKa) durch hochqualifizierte Täter unter Nutzung modernster Technologien stattgefunden hat. Beim zweiten Angriff wurde diese noch ergänzt durch eine Desinformationskampagne von gesteuerten „Influencern".

Die Ausprägung der eigenen Fähigkeiten:

Fähigkeitskategorien Schutz und Resilienz	In diesem Anwendungsfall derzeit vorhanden	Ausgewählte künftig anzustrebende Erweiterungen/Ergänzungen
Prävention	Schritte angestoßen; noch Nachholbedarf bei Bund/Ländern/Kommunen	OSINT-Aufklärung; „Digital Listening" Plattform zur Bedrohungsfrüherkennung; Interdisziplinäres Lagebild in Echtzeit Ggf. EloKa-Schutzmaßnahmen (Elektronische Kampfführung)
Detektion	Schritte angestoßen; noch Nachholbedarf bei Bund/Ländern/Kommunen	Ggf. Videokameras; Ggf. Einsatz von Aufklärungsdrohnen
Intervention	Feuerwehr und Polizei sind nach Alarmierung rasch vor Ort	Interdisziplinäres Lagebild in Echtzeit
Stabilisierung	Umleitungen für den Bahnverkehr und für den Straßenverkehr	Leistungsfähiges Business Continuity-Konzept mit Redundanz-Planung, Ersatzteil-Bevorratung, Ressourcen zur Schnellinstandsetzung etc. Ggf. nationales „Pooling & Sharing"-Konzept; Ggf. Standardisierung von (technischen) Bauteilen

6.4.6 Grenzen klassischer Standortsicherheitskonzepte – Schutz vs. Resilienz

Ein großer Teil der Kritischen Infrastrukturen kann nicht klassisch durch eine Rundumsicherung beziehungsweise durch Umzäunen und so weiter geschützt werden. Hochspannungsleitungen, Pipelines, Autobahnen, Eisenbahnlinien und Ähnliches zählen zu dieser „Kategorie B" von KRITIS (vgl. Kapitel 6.4.2 – Seite 52 ↗).

Hier sind die Schutzziele (2), (3) und (4) nicht zu erreichen.

Ein weiterer großer Teil der KRITIS kann zwar klassisch durch Umzäunung und Ähnliches geschützt werden, liegt aber so entlegen beziehungsweise fernab, dass professionelle Interventionskräfte nicht so kurzfristig nach Alarmierung vor Ort sein können, wie dies die Logik der Widerstandszeiten erfordert. Beispielsweise ein Umspannwerk im Wald, ein Wasserkraftwerk am Fluss oderein Windrad zählen zur „Kategorie A2" (vgl. Kapitel 6.4.2 – Seite 52 ↗).)

Hier sind die Schutzziele (5) und (6) nicht zu erreichen.

Dann muss davon ausgegangen werden,

- dass sich ein begonnener Angriff nicht verhindern und in seinem Verlauf nicht beeinflussen lassen wird,
- dass ein Angreifer weitgehend ungehindert an und in das Objekt gelangen und an die kritischen Einrichtungen oder Anlagen vordringen können wird.

Dies erfordert eine Fokussierung auf die Fähigkeiten zur Stabilisierung, das heißt Gegenmaßnahmen, Notbetrieb, Einsatz von Reserven, Nutzung von Redundanzen, Instandsetzung und die Wiederherstellung des Normalbetriebs.

Daher sollte insbesondere bei Kritischen Infrastrukturen der „Kategorie A2“ und der „Kategorie B“ angestrebt werden, die Fähigkeiten zur Stabilisierung auszubauen, um die Schutzziele (7), (8), (9) und (10) zu erreichen.

Hier sollte sich somit das Augenmerk verschieben – weg vom „Schutz“ der einzelnen Anlage oder Einrichtung, der nicht wirklich zu gewährleisten ist – hin zur Aufrechterhaltung der benötigten (Dienst-)Leistungen beziehungsweise zur „Resilienz“, auf die es eigentlich ankommt!

Die im Rahmen des Ausgangsszenars 2030 zu erwartenden hohen Bedrohungsintensitäten unter anderem durch Terroristen und militärische Spezialkräfte erfordern ohnehin eine Neuorientierung.

> Anstelle der „klassischen“ Standortsicherheitskonzepte (mit Fokus unter anderem auf die DIN EN 1627) werden hier ganzheitliche Schutzkonzepte nach dem Allgefahrenansatz benötigt, die auf eine unterbrechungsfreie Fortführung der zentralen Geschäfts- und Verwaltungsaktivitäten abzielen – unabhängig von Art und Ursache der möglichen Störereignisse.

6.4.7 Verwaltung als Kritische Infrastruktur

Aktuelle und vergangene Krisen haben gezeigt, dass die Zusammenarbeit zwischen Ressorts auf Ebene der Länder und des Bundes und darüber hinaus zwischen den Akteuren von Bund und Ländern durchaus herausfordernd sein kann.

Gründe hierfür können sein:

- **Kompetenzüberschneidungen und Kompetenzkonflikte**, die zu Verzögerungen und Ineffizienz führen.
- **Unterschiedliche Verwaltungsstrukturen und IT-Systeme**, die den Informationsaustausch und die Koordination behindern.
- **Langwierige Entscheidungsprozesse** aufgrund des Konsensprinzips und divergierender politischer Interessen.
- **Schwache Kommunikation und Koordination**, die zu Missverständnissen und ineffizienten Abläufen führt.
- **Finanzielle Ungleichheiten** und Abhängigkeiten, die Spannungen zwischen Bund und Ländern schaffen.
- **Mangel an Ressourcen** und Fachkräften, der die Zusammenarbeit bremst.
- **Politische und kulturelle Differenzen**, die Zusammenarbeit erschweren.
- **Bürokratische Hürden und starre Strukturen**, die Flexibilität und Geschwindigkeit mindern.

Kommunikation erfolgt vertikal zwischen den Ressorts beziehungsweise auch vertikal über Ebenen hinweg. Eine Koordination gibt es in der Regel nicht. Informationsdefizite sind vorprogrammiert. Ein gemeinsames Lagebild zu erstellen, ist schwerlich möglich.

Zuständigkeiten: Kommunikationsstränge vertikal und horizontal

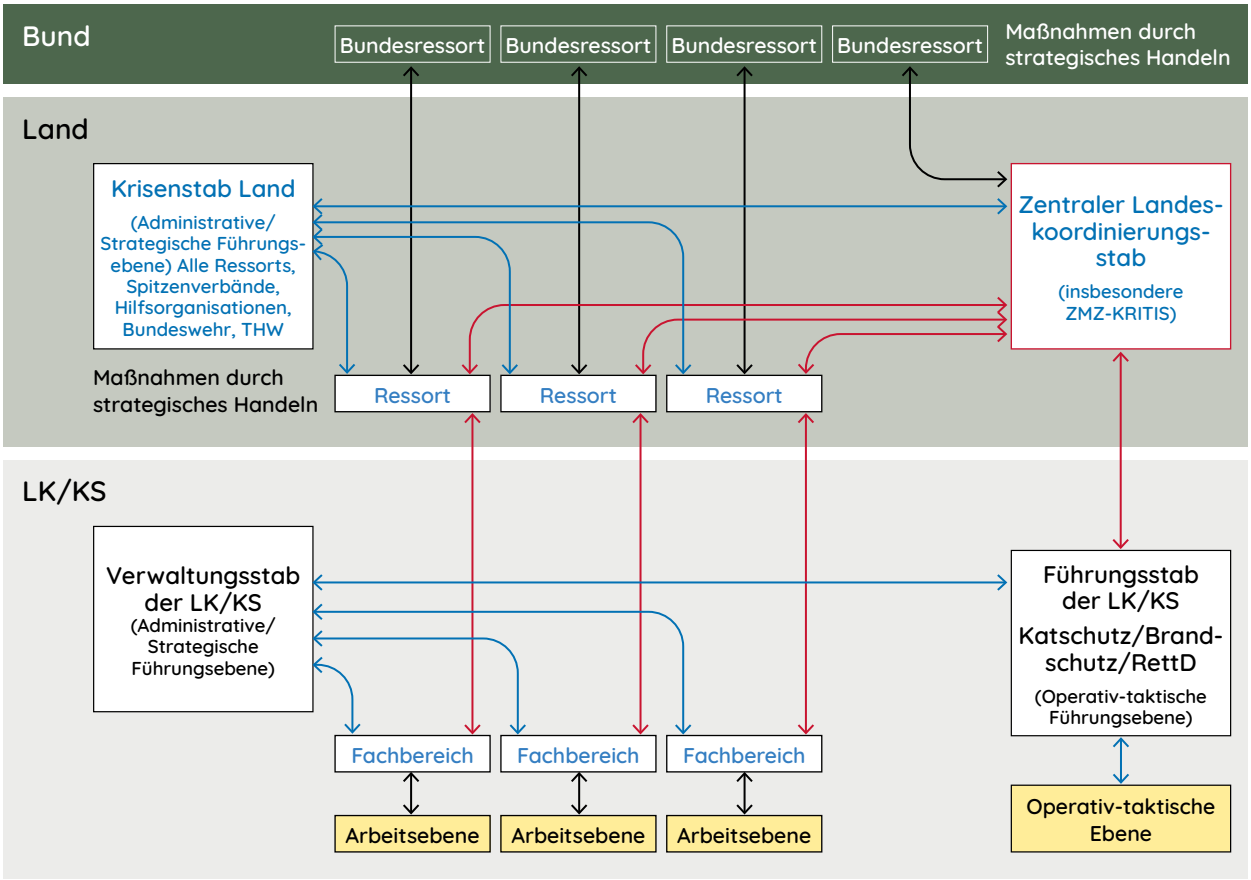

Abbildung 11: Die Grafik veranschaulicht exemplarisch die vertikalen und horizontalen Kommunikationswege, die genutzt werden.

Zentrale Koordinierungsstäbe auf Landes- und Bundesebene könnten aus dem Dilemma helfen (vgl. Abb. 11). Sie sorgen für einen geordneten Informationsaustausch zwischen den einzelnen Ressorts.

Voraussetzung dafür ist, dass sich die Ressorts dieser Struktur unterwerfen und jeweils einen Single Point of Contact (SPOC) einrichten.

Es ist ratsam, diese Art der Zusammenarbeit in einer Gemeinsamen Geschäftsordnung (GGO) zu regeln. Eine solche GGO sollte innerhalb eines Landes einen bestimmten Status aktivieren.

Da sich das Katastrophenschutzrecht der Länder in der Regel nur auf regionale und selten auf ressortübergreifende Ereignisse bezieht, ist es nur bedingt geeignet.

6.4.8 Erkenntnisse in Bezug zu der Bearbeitung der KRITIS-Anwendungsfälle

In den dargestellten KRITIS-Anwendungsfällen zeigt sich ein wiederkehrendes Muster, aus dem sich die folgenden Maßnahmen und **Handlungsnotwendigkeiten** ergeben:

- Grundsätzlich: Je höher die Intensität des Angriffs ist, desto weniger sind die klassischen Standortsicherheitsmaßnahmen ausreichend und umso wichtiger werden angemessene BCM-Konzepte beziehungsweise ein **Fokus auf die Resilienz der KRITIS**.
- Ein **interdisziplinäres Lagebild in Echtzeit** könnte den relevanten Akteuren, insbesondere bei überregionalen Ereignissen und Parallel-Ereignissen, die Lageführung und damit die Schadensbegrenzung, den Notbetrieb

und die Koordination von Instandsetzungsmaßnahmen zur Wiederherstellung des Normalbetriebs wirkungsvoll unterstützen (siehe Grünbuch „Interdisziplinäres Lagebild in Echtzeit“ des ZOES e. V. vom März 2023).

- Eine geeignete **Plattform zur Bedrohungsfrüherkennung als Bestandteil eines interdisziplinären Lagebildes in Echtzeit** könnte Grundlage sein für ein gemeinsames Sicherheitslagebild, mit dem die relevanten Akteure „vor die Lage kommen“ (vgl. „Eckpunkte der Nationalen Wirtschaftsschutzstrategie“ des BMI vom Februar 2024).

- Erstellung eines **ganzheitlichen Raum- und Objektschutzkonzeptes** für alle Bundesländer: Hierbei wären idealerweise die Hauptverwaltungsbeamten zu beteiligen, die in ihrem jeweiligen Verantwortungsbereich die Kritischen Infrastrukturen erfassen und im Hinblick auf deren Kritikalität und Schutzbedarf katalogisieren. Angemessene Maßnahmen zur Stärkung der Resilienz von Wirtschaft und Verwaltung und zur Unterstützung der Zivil-Militärischen Zusammenarbeit (ZMZ) könnten auf dieser Grundlage geplant und umgesetzt werden. Eine entsprechende Rechtsnorm auf Länderebene ist notwendig.

- Bestehende Prozesse und Methoden zur Krisenbewältigung sind zu prüfen und gegebenenfalls weiterzuentwickeln, insbesondere im Hinblick auf den Allgefahrenansatz und die Herausforderungen durch mehrere in unterschiedlichen Bundesländern zeitgleich stattfindende Schadensereignisse auch infolge doloser Handlungen von hoher Intensität.

- Planspiele, Übungen und die Nutzung neuer Technologien:

  - Gute Ansätze verfolgt die **L**änder- und Ressort**ü**bergreifende **K**risenmanagementübung (**Ex**ercise), Übungsserie **LÜKEX**. Ihr Ziel ist es, die Zusammenarbeit und Koordination von Behörden und Organisationen auf allen föderalen Ebenen (Bund, Länder, Kommunen), Unternehmen sowie zwischen zivilen und militärischen Kräften im Krisen- und Katastrophenfall zu testen und zu verbessern.
  - War Games sind unter anderem bei der Analyse von Krisen- und Konfliktszenarien ein wichtiges Instrument, um die komplexe Dynamik von Entscheidungssituationen zu verstehen und Handlungsstrategien zu optimieren. Sie bieten ein sicheres Umfeld, um Risiken und Chancen auszuloten, bevor sie in der realen Welt getestet werden.
  - Neue Technologien wie zum Beispiel der Einsatz von Künstlicher Intelligenz (KI) oder Simulationsunterstützung durch „Digitale Zwillinge“ sind mit Blick auf die Bedeutung ziviler Infrastrukturen für die Unterstützung der Streitkräfte mit einzubeziehen.
  - Bestehende Verantwortlichkeiten sind zu überprüfen und gegebenenfalls neu festzulegen. Eine oder ein ZMZ-Beauftragter auf Bund- und Länderebene ist zu ernennen. Diese oder dieser kann als Fachberaterin oder Fachberater ZMZ in den jeweiligen Koordinierungsstäben installiert sein. Dabei bleiben Ressortzuständigkeiten auf allen Ebenen erhalten.

- Durch zusätzliche Aufgaben wird ein zusätzlicher Personal- und Fähigkeitsbedarf entstehen – dementsprechend sind geeignete Einsatzkräfte auszuwählen, einzustellen und auszubilden; außerdem ist die Bevölkerung für angemessenes Handeln in einer sich verschärfenden Sicherheitslage zu sensibilisieren (gesamtgesellschaftliche Aufgabe).

- Ressortübergreifende Zuständigkeiten erschweren ein koordiniertes Verwaltungshandeln. Eine Lösung stellt eine gemeinsame Geschäftsordnung (GGO) dar. Eine GGO der Ministerien und der Staats- oder Senatskanzleien zur Zusammenarbeit bei Krisen und Katastrophen regelt die bei Krisen und Katastrophen geltenden Grundsätze der Organisation, der Zusammenarbeit und des Geschäftsganges der Ministerien und des Geschäftsbereichs der Ministerpräsidentin oder des Ministerpräsidenten – Staatskanzlei/Senats-

kanzlei – sowie des Geschäftsverkehrs nach außen. Die Geschäftsordnung ist für alle Ministerien und die Staatskanzleien auf Landesebene und die Ministerien auf Bundesebene und das Bundeskanzleramt verbindlich.

- Innerhalb der Verwaltung sollte eine präzise Abgrenzung von Zuständigkeiten mögliche Kompetenzkonflikte vermeiden.

- **Digitalisierung und Harmonisierung von IT-Systemen**: Der Ausbau interoperabler Systeme und digitaler Plattformen verbessert den Informationsaustausch.

- **Effizientere Entscheidungsprozesse**: Abbau von bürokratischen Hürden und eine bessere Abstimmung auf allen Ebenen könnten die Entscheidungsfindung beschleunigen, bedarfsweise durch die Nutzung des Pareto-Prinzips (80 Prozent des Ergebnisses können in der Regel durch 20 Prozent des Aufwandes erreicht werden).

- **Finanzielle Reformen**: Anpassungen im Finanzausgleich und eine gerechtere Berücksichtigung der Mittel für ein adäquates Krisenmanagement können Spannungen reduzieren.

- **Schulungen und Austauschprogramme**: Bessere Schulung und fachlicher Austausch zwischen den Ebenen stärken die Zusammenarbeit (jeder und jede Mitarbeitende in der Verwaltung ist auch Krisenmanager beziehungsweise Krisenmanagerin).

- Der Begriff „Krise“ sollte als Ereigniszustand, ähnlich wie der Begriff „Katastrophe“, etabliert werden (Feststellung durch das Kabinett).

- Gesetze und Verordnungen sollten schon in der Entstehungsphase auf „ZMZ-Tauglichkeit“ geprüft werden, mögliche Regelungslücken sind zu schließen.

6.4.9 Der Beitrag der Sicherheitswirtschaft beim Schutz Kritischer Infrastrukturen

Private Sicherheitsdienstleister in Deutschland beschäftigen bundesweit rund 285.000 Sicherheitsmitarbeiterinnen und -mitarbeiter und erbringen seit Jahren immer mehr Tätigkeiten, die der Absicherung beziehungsweise Aufrechterhaltung von sämtlichen KRITIS-Sektoren in Deutschland dienen. Dazu zählen Objektschutzaufgaben bei Kraftwerken, Schutz von Lieferketten, Sicherstellung der Bargeldversorgung, Gewährleistung von Sicherheit und Ordnung im Personenverkehr und Durchführung von Luftsicherheitskontrollen. Das Sicherheitsgewerbe als Teil der nationalen Sicherheitsarchitektur ist bereits heute – ohne selbst als eigenständiger KRITIS-Sektor zu gelten – faktisch integraler Bestandteil beim Schutz sämtlicher KRITIS-Sektoren und KRITIS-Anlagen. Das Sicherheitsgewerbe trägt damit maßgeblich dazu bei, dass unbefugte Personen KRITIS-Anlagen nicht betreten, um dort insbesondere Sabotage- und Terrorangriffe durchzuführen. Gerade im Bereich der Bewachung militärischer Liegenschaften ist für mehr als 7.000 Beschäftigte eine erweiterte Sicherheitsüberprüfung (SÜ) gemäß § 9 SÜG (sogenannte Ü2) notwendig. Insofern ist das Sicherheitsgewerbe bedeutend für die Resilienz von KRITIS-Anlagen in Deutschland.

Hieraus leiten sich folgende Handlungsnotwendigkeiten ab:

1. Die bundesweite rechtliche Verankerung der besonderen Bedeutung des Sicherheitsgewerbes ist dringend erforderlich, um in allen zukünftigen Sicherheitslagen den Schutz der Kritischen Infrastrukturen (KRITIS) und systemrelevanter Betriebe gewährleisten zu können.

2. Für den Fall, dass Sicherheitsunternehmen oder (interne oder externe) Sicherheitsmitarbeiter in die Sicherung kritischer Anlagen eingebunden sind, bedarf es zwingend derselben gesetzlich vorgegebenen Leistungs- und Sicherheitsstandards.

3. Vor dem Hintergrund der veränderten Sicherheitslage und den damit gestiegenen Gefahren durch Spionage und Sabotage ist das Sicherheitsüberprüfungsgesetz (SÜG) in Teilen zu verändern und die aktuell viel zu lange durchschnittliche Bearbeitungsdauer von Sicherheitsüberprüfungen durch massiven Personalzuwachs signifikant zu verkürzen.

4. „Doppelüberprüfungen" von Sicherheitspersonal sollten aus Gründen der Datensparsamkeit, aus Gesichtspunkten des Bürokratieabbaus und insbesondere auch aus Gesichtspunkten der SÜ-Verfahrensbeschleunigung reduziert werden.

7 Handlungsempfehlungen

- Die Weiterentwicklung und Steuerung der Zivil-Militärischen Zusammenarbeit (ZMZ 4.0) erfordert die Einrichtung von ZMZ-Koordinatoren auf Bundes-, Landes- und kommunaler Ebene, denen Rechte, Befugnisse zuzuweisen und Verantwortlichkeit zu übertragen sind.

- Das Bewusstsein für die veränderte Bedrohungslage ist in der Gesellschaft, in den Verwaltungen und in den Parlamenten durch adressatengerechte Information zu schärfen, damit die jeweils eigene Verantwortung verinnerlicht wird.

- Wirksame ZMZ 4.0 ist handlungsleitend für Entscheidungsträger und Entscheidungsträgerinnen in Politik, Verwaltung und Wirtschaft, um mögliche Aggressoren abzuschrecken, die Bundesrepublik Deutschland verteidigen zu können und die freiheitlich demokratische Grundordnung zu schützen.

- Zivil-Militärische Zusammenarbeit muss auf allen Ebenen von Politik, Verwaltung, Wirtschaft und Bevölkerung als gesamtgesellschaftliche Aufgabe verstanden werden. Deshalb ist ZMZ bereits in Schulen zu vermitteln und mit relevanten Akteuren regelmäßig zu üben.

- Gesetze und Verordnungen sind im Hinblick auf wirksame ZMZ 4.0 zu überprüfen und eventuelle Regelungslücken zu schließen.

- Erstellung eines einheitlichen Bundeslagebildes. Das GRÜNBUCH „Lagebild“ enthält hierfür die Lösungsvorschläge. https://zoes-bund.de/gruenbuch-lagebild/

- Erstellung eines Raum- und Objektschutzkonzeptes auf Grundlage einer Risikobetrachtung unter dem Gesichtspunkt von Leistungsfähigkeit und Resilienz der Gesamtverteidigung.

- Auf allen Ebenen sind die Haushaltsansätze auch auf die ZMZ 4.0 auszurichten.

8 Schlussbetrachtung und Ausblick

Die Zivil-Militärische Zusammenarbeit (ZMZ) bedarf einer schnellen Anpassung an die veränderte Bedrohungslage.

Die dauerhafte Hybride Bedrohung Deutschlands – durch Cyberangriffe, Desinformationskampagnen, wirtschaftliche Erpressung, Sabotage, Spionage und andere nichtmilitärische Mittel – erfordert eine umfassende und nachhaltige Reaktion. Erforderlich sind bereits im Vorfeld einer militärischen Krise zentrale Konsequenzen, die daraus gezogen werden sollten:

1. Stärkung der Resilienz

- **Sensibilisierung der Gesellschaft**: Schulungen und Aufklärungsprogramme, um Bevölkerung und Unternehmen für Desinformation und Cyberrisiken zu sensibilisieren.
- **Cybersicherheit ausbauen**: Ausbau der technischen und organisatorischen Sicherheitsmaßnahmen, vor allem in Kritischen Infrastrukturen (Energie, Gesundheit, Verkehr, Kommunikation). Investitionen in moderne Technologien wie durch Künstliche Intelligenz gestützte Erkennung von Cyberangriffen, sind notwendig.
- **Business Continuity Planung**: Analyse der Resilienz-Risiken insbesondere für die Kritischen Infrastrukturen nach dem Allgefahrenansatz und Erarbeitung ganzheitlicher, integrierter Resilienzkonzepte für Staat, Wirtschaft und Gesellschaft.
- **Förderung strategischer Autonomie**: Reduzierung der Abhängigkeit von Lieferketten, Technologien und Energie aus potenziell feindlich gesinnten Staaten.

2. Gesellschaftlicher Zusammenhalt

- **Demokratieförderung**: Stärkung demokratischer Institutionen und des Vertrauens in den Staat, um die Gesellschaft widerstandsfähiger gegen Manipulationen zu machen.
- **Medienkompetenz fördern**: Investitionen in Bildung, um die Fähigkeit der Bürger zu stärken, zwischen seriösen und manipulativen Informationen zu unterscheiden.

3. Ausbau der Sicherheitsstrukturen

- **Verstärkung der Nachrichtendienste**: Ausbau der Kapazitäten des Bundesamtes für Verfassungsschutz (BfV), des Bundesnachrichtendienstes (BND) und des Bundesamtes Militärischer Abschirmdienst (BMAD) zur Identifikation und Abwehr Hybrider Bedrohungen.
- **Koordinierte Zusammenarbeit**: Schaffung einer zentralen Koordinationsstelle für hybride Gefahren, die alle relevanten Behörden und Ministerien einbindet.

4. Abschreckung und Gegenmaßnahmen

- **Physischer und digitaler Grundschutz**: Aufbau von Mindestfähigkeiten von Kritischen Infrastrukturen zu Selbstschutz und Resilienz gegenüber Angriffen in der physischen und der digitalen Welt.
- **Offensive Cyberfähigkeiten**: Aufbau und Einsatz von Fähigkeiten zur Abwehr und Gegenschlägen im Cyberraum, um Angreifer aktiv zu stören.
- **Sanktionen und rechtliche Maßnahmen**: Schärfere Sanktionen gegen Staaten oder Akteure, die hybride Angriffe fördern oder durchführen.
- **Strategische Kommunikation**: Aufbau von Kapazitäten für eine proaktive Informationspolitik, um Desinformationskampagnen frühzeitig zu entlarven und entgegenzuwirken.

5. Rechts- und Rahmenbedingungen anpassen

- **Anpassung des rechtlichen Rahmens**: Modernisierung von Gesetzen, um hybride Angriffe rechtlich besser zu fassen und effektiver zu ahnden.

- **Regulierung von Technologien**: Einführung von Standards und Gesetzen, die den Missbrauch moderner Technologien (zum Beispiel Künstliche Intelligenz, Deepfakes) verhindern.

- **Schutz der Meinungsfreiheit**: Gleichzeitige Sicherung demokratischer Grundrechte, um Missbrauch bei Maßnahmen gegen Desinformation zu vermeiden.

Die dauerhafte Hybride Bedrohung erfordert im Sinne des Schutzversprechens des Staates gegenüber seinen Bürgerinnen und Bürgern eine ganzheitliche Sicherheitsstrategie, die sowohl technische, organisatorische als auch gesellschaftliche Maßnahmen umfasst. Dabei muss der Staat flexibel und proaktiv handeln, um mit den sich schnell wandelnden Bedrohungen Schritt zu halten, ohne dabei grundlegende Werte wie Freiheit und Demokratie zu gefährden. Die Stärkung der Resilienz und die Förderung internationaler Zusammenarbeit sind Schlüssel zur langfristigen Sicherheit Deutschlands.

QUELLEN UND ERLÄUTERUNGEN

1 Vgl. Freudenberg, Dirk/von Lewinski, Kai: Handbuch Bevölkerungsschutz. München, C.H. Beck, 2024.

2 Bundesministerium des Innern und für Heimat (BMI): „System des Krisenmanagements in Deutschland“, in: BMI, 2015, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/krisenmanagement-in-deutschland.pdf?__blob=publicationFile&v=1 (abgerufen am 20. Oktober 2024).

3 Vgl. Depenheuer, Otto, in Maunz/Dürig, Grundgesetz-Kommentar, 80. Ergänzungslieferung, 2017, Art. 80a GG, Rn. 69.

4 North Atlantic Treaty Organization: „The North Atlantic Treaty“, in: NATO, 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm (abgerufen am 20. Oktober 2024)

5 Bundeswehr: „Operatives Führungskommando der Bundeswehr“, in: Bundeswehr, 2024, https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/operatives-fuehrungskommando-der-bundeswehr (abgerufen am 20. Oktober 2024).

6 Schmid, Johann, „Kriegsbild und hybride Kriegführung – Ableitungen für die Verteidigung“, in: ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 958, 2023, S. 2.

7 Anmerkung der verfassenden Person: Das Joint Research Center der Europäischen Kommission definiert diese exemplarisch als „Kombination verschiedener Arten von Instrumenten, von denen einige erwartet und bekannt sind, während andere unerwartet und heimlich eingesetzt werden, um ein nicht deklariertes strategisches Ziel zu erreichen, ohne dies offiziell zuzugeben.“ European Commission, Joint Research Centre: „Hybrid Threats. A Comprehensive Resilience Ecosystem“, in: European Commission, 2023, S. 5, https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en?prefLang=de&etrans=de (abgerufen am 20. Oktober 2024)

8 Anmerkung der verfassenden Person: Das US-amerikanische Argonne National Laboratory kommt zu einer ähnlichen Schlussfolgerung und definiert diese als „solche, die von Gegnern ausgehen, die in der Lage sind, gleichzeitig konventionelle und nicht-konventionelle Mittel adaptiv einzusetzen, um ihre Ziele zu verfolgen.“ Argonne National Laboratory: „Combating Hybrid Threats“, in: Argonne National Laboratory, https://www.anl.gov/partnerships/combating-hybrid-threats (abgerufen am 20. Oktober 2024)

9 Anmerkung der verfassenden Person: Im Kontext der NATO werden diese zumeist definiert als „eine Art von Bedrohung, die konventionelle, irreguläre und asymmetrische Aktivitäten in Zeit und Raum kombiniert." Civil-Military Cooperation Centre of Excellence: „Hybrid Threats“, in: Civil-Military Cooperation Centre of Excellence, 2024, https://www.cimic-coe.org/cimic/Definitions/Hybrid-Threats/ (abgerufen am 20. Oktober 2024)

10 Vgl. Bundesministerium der Verteidigung (BMVg): „Hybride Bedrohungen“, in: Bundesministerium der Verteidigung, https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen (abgerufen am 20. Oktober 2024)

11 Innenministerkonferenz (IMK): „Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 219. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder“, in: IMK, 2023, https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/20230616_14.html?nn=4812206 (abgerufen am 20. Oktober 2024).

12 Bundesministerium des Innern und für Heimat (BMI): „Desinformation als hybride Bedrohung“, in: BMI, 2023, https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation/artikel-desinformation-hybride-bedrohung.html (abgerufen am 20. Oktober 2024).

13 Szenare sind gängige Praxis in Streitkräften, anderen Sicherheitsorganen, in Behörden und Unternehmen oder der Wissenschaft. Wesentliche Ziele sind
1. Vorstellungen von künftigen Entwicklungen und von deren Einflussfaktoren zu gewinnen,
2. Komplexität und Abhängigkeiten zu erkennen,
3. Entscheidungsbedarf im Prozessablauf zu ermitteln,
4. Kompetenzen zuzuschreiben, Ressourcen zu planen und Akteure zu koordinieren,
5. Prozesse zu trainieren sowie
6. Strategien zu entwickeln und zu überprüfen.
Szenare sind keine Vorausschau oder Vorhersagen. Sie sind auf ein spezifisches und eingegrenztes Erkenntnisinteresse fokussiert und skizzieren dafür fiktive, aber abstrakt mögliche und in sich plausible Situationen und Ereignisfolgen.

14 Ausgehend von diesen Zahlen bedeutet dies unter heutigen notfallmedizinischen Bedingungen, dass täglich mindestens 336 Rettungswagen mit Notarzt, 220 Notfallkrankenwagen und etwa 220 Krankenwagen benötigt werden, die zusätzlich zu den Regelrettungsdiensten in Dienst gestellt werden müssten. Dabei sind Weiterverlegungen dieser Patientinnen und Patienten in Weiterbehandlungs- und Rehabilitationseinrichtungen nicht eingerechnet.

IMPRESSUM

Zukunftsforum Öffentliche Sicherheit e. V.

Friedrichstraße 95
10117 Berlin
Telefon +49 30 20 64 17 17
Telefax +49 30 20 64 17 16

info@zukunftsforum-oeffentliche-sicherheit.de
www.zukunftsforum-oeffentliche-sicherheit.de

Vorstand

Albrecht Broemme, Vorsitzender
Dr. Claudia Thamm, Stellv. Vorsitzende
Stephan Boy, Schatzmeister
Michael Bartsch
Wolfgang Lohmann
Frank Weber

Redaktionelle Begleitung

Karl-Heinz Aufmuth
Robin Bangard
Fabian Hemker
Daniel Lücking
Nils Lüttschwager
Sönke Jacobs

Organisation

Daniela Teichert

Gestaltung

Regina Kramer
www.skaadoosh.de

Druck

DCM Druck Center Meckenheim GmbH
www.druckcenter.de

Berlin, 1. Auflage Januar 2025

Zukunftsforum
Öffentliche Sicherheit