

GESAMT- STAATLICHES SICHERHEITS- ÖKOSYSTEM 2030.

» Sicherheit entsteht **nicht** in Silos.

STRATEGIC PARTNER

AS ARVATO SYSTEMS Google Cloud

SOLUTION PARTNER

AIRBUS  bechtle CGI secunet

SUPPORTING PARTNER

conet infodas  msg soffico sopra 



Ron Simon
AFCEA Bonn e.V.
Programm und Konzeption



Jochen Reinhardt
AFCEA Bonn e.V.
Programm und Konzeption



Gunnar Sohn
Smarter Service Institut
Lektorat



Bernhard Steimel
mind digital
Studienleiter

Impressum

Herausgeber

AFCEA Bonn e.V. · Borsigallee 2 · 53125 Bonn · Telefon +49 228 925 82 52 · buero@afcea.de · www.afcea.de

Eingetragen beim Amtsgericht Bonn, VR 5105 · USt-IdNr. DE 123 381 970. Vertretungsberechtigter Vorstand: Armin Fleischmann (Vorsitzender), Ron Simon, Marc Akkermann. Verantwortlich im Sinne des Presserechts ist Jochen Reinhardt, Anschrift wie oben.

Bibliografische Angaben

Gesamtstaatliches Sicherheitsökosystem 2030 · Sicherheit entsteht nicht in Silos · 1. Auflage · Bonn, Oktober 2026.

Druckausgabe: Herstellung und Vertrieb im Print-on-Demand-Verfahren über Amazon.

Digitale Ausgabe: kostenfrei unter www.afcea.de.

Zitiervorschlag: AFCEA Bonn e.V. (Hrsg.) (2026): Gesamtstaatliches Sicherheitsökosystem 2030 · Sicherheit entsteht nicht in Silos, Studienleitung: Bernhard Steimel. Bonn.

Mitwirkende

Studienleitung und Redaktion: Bernhard Steimel, mind digital · Programm und Konzeption: Ron Simon · Jochen Reinhardt, AFCEA Bonn e.V. · Lektorat: Gunnar Sohn, Smarter Service Institut · Gestaltung und Satz: Ernst Merheim

Partner der Studie

Strategic Partner Arvato Systems · Google Cloud

Solution Partner Airbus · AWS · Bechtle · CGI · secunet

Supporting Partner conet · infodas · msg · MilDef · soffico · Sopra Steria

Die Zwischenstände wurden in drei Expertenworkshops mit Vertreterinnen und Vertretern der Studienpartner geprüft.

Rechtliches

© 2026 AFCEA Bonn e.V. Diese Studie erscheint unter der Lizenz Creative Commons CC BY-ND 4.0: Weitergabe und Vervielfältigung sind bei Nennung der Quelle erlaubt, Veränderungen nicht.

Die Studie verweist auf externe Websites. AFCEA Bonn e.V. hat auf deren Inhalte keinen Einfluss und übernimmt dafür keine Haftung.

Bildnachweise: Titel: KI-generiert DALL-E · Porträts der Beteiligten: die abgebildeten Personen oder ihre Organisationen · Grafiken: AFCEA Bonn e.V.

STRATEGIC PARTNER



SOLUTION PARTNER



SUPPORTING PARTNER



Gesamtstaatliches Sicherheitsökosystem 2030

Deutschland hat die Mittel, die Fähigkeiten und die Menschen, um 2030 in Krisen und Sicherheitslagen handlungsfähig zu sein. Zwischen Behörden, Ebenen und Systemen reißt die Handlungskette jedoch regelmäßig ab – vor, während und nach solchen Lagen. Diese Studie zeigt, wo die Schwächen liegen und welche Maßnahmen ein funktionierendes gesamtstaatliches Sicherheitsökosystem erreichbar machen.

Wie diese Studie aufgebaut ist

Die Untersuchung identifiziert Bedarfe und Anforderungen an ein gesamtstaatliches Sicherheitsökosystem und formuliert sie als **Wirkungsversprechen**. Daraus leiten sich fünf **Kernbefunde** ab, die beschreiben, was heute nicht funktioniert (Seite 10). Das **Zielbild** übersetzt sie in eine Sicherheitsarchitektur: Sie gibt den Handlungsfeldern Struktur und ihren Platz im Ökosystem (Kapitel 3). **Kapitel 4** klärt **Mandat und Rollen**, Kapitel 5 das **digitale Rückgrat**, auf dem alles aufsetzt. Wie weit Deutschland dabei ist, misst der **Systemreife-grad-Benchmark** über zehn Dimensionen und sechs Länder (Abschnitt 3.5). Was der Markt dazu heute anbietet, prüft Kapitel 6 als **Fähigkeitsbeitrag**. Daraus leitet die Studie 30 **Maßnahmen** mit Träger, Frist und Nachweis ab (Kapitel 7).

Woher die Zahlen kommen

Vier Erhebungen bilden die Grundlage dieser Studie.

1. 55 Tiefeninterviews mit 61 Gesprächspartnern aus Behörden, Kommunen, Streitkräften, Wirtschaft und Wissenschaft, von März bis Juni 2026. Davon wurden 50 Interviews quantitativ ausgewertet.
2. Eine Online-Befragung unter 72 Anbietern und Anwendern.
3. Ein Systemreifeegrad-Vergleich über zehn Dimensionen und sechs Länder.
4. Eine Auswertung bestehender Studien, Regierungsberichte und Rechtsgrundlagen.

Daraus entstanden drei Datenbanken mit 105 Praxisbeispielen, 172 Lösungen und 529 Vorschlägen. Der internationale Vergleich folgt derselben Logik: aus den Studien die Kriterien, aus den Kriterien die zehn Dimensionen, aus Interviews und Befragung ihre Bewertung. Er ist hergeleitet, nicht behauptet.



Was belegt ist und was aussteht

Woher die Zahlen stammen. Zahlen ohne Quellenangabe stammen aus der eigenen Erhebung. Marktaussagen stützen sich auf Angaben der Online-Befragung und Interviews, Aussagen über den Bestand auf alle 172 Lösungen. Prozentwerte beziehen sich auf die Zahl der Nennungen, nicht auf die Zahl der Befragten.

Wie belastbar die Angaben sind. Jede Aussage stützt sich auf ein Gespräch, eine Befragung oder eine benannte Quelle, das Quellenverzeichnis beginnt auf **Seite 116**. Offen ist allein der Peer-Review des internationalen Vergleichs, zwei der zehn Dimensionen tragen bewusst keinen Wert. Wie die Studie entstanden ist und wo ihre Grenzen liegen, beschreiben die **Seiten 112** und 113.

Wo Begriffe erklärt werden. Das **Glossar** beginnt auf Seite 114.

Wo Sie einsteigen

Sie entscheiden über Mandate, Haushalte oder Gesetze. Kapitel 4 und 7 zeigen, welche drei Entscheidungen die Mandatslücken schließen und woran sich die Wirkung nach zwölf Monaten messen lässt.

Sie führen im Ernstfall in einer Behörde, einer Leitstelle oder einem Kommando. Kapitel 1 bis 4 zeigen, wo die Handlungskette abreißt und welche sechs Rollen das Gefüge tragen. Zwei davon haben bis heute kein Mandat.

Sie bauen, betreiben oder erforschen Technik für den Ernstfall.

Kapitel 5 und 6 prüfen dreizehn Fähigkeitsbeiträge am Zielbild und zeigen, für welche Technologie-Domänen es derzeit keine Lösung gibt.

Sie sind Bürgerin oder Bürger und wollen wissen, wie Sie mitwirken können. Kapitel 2 zeigt, was getragen hat. Kapitel 7 beschreibt, was die Bevölkerung beitragen kann und was in den ersten 72 Stunden bei Ihnen selbst liegt.

Grußwort 8 Prolog 9 Management Summary 10 Handlungsfelder 11

01 · Gesamtstaatliche Sicherheit 12

Zeit wird zur kritischen Variable
Nicht die Fähigkeit fehlt, sondern die Kopplung.

02 · Lernen aus der Praxis 23

Wo Handlungsfähigkeit abreißt
Fünf Lagen gelangen, drei nicht – die Ursache wiederholt sich.

03 · Das Zielbild 32

Ein Sicherheitsökosystem, das Wirkung erzielt
Deutschland liegt mehr als zehn Jahre zurück.

04 · Governance first 45

Ohne Orchestrierung keine Wirkung
Sechs Rollen tragen das Gefüge, zwei ohne Mandat.

05 · Das digitale Rückgrat 59

Kopplungsfähigkeit statt einer Plattform
Für drei von acht Domänen liefert der Markt nichts.

06 · TechKompass 71

Fähigkeitsbeiträge zum Sicherheitsökosystem 2030
Fähigkeitslücken bis 2030 schließen.

07 · Von der Vision zur Umsetzung 94

Wie Deutschland handlungsfähiger wird
Dreißig Maßnahmen, sechs priorisiert.

Epilog 110 Über diese Studie 111

BETEILIGTE

Wer diese Studie trägt

Diese Studie beruht auf Gesprächen mit Menschen, die im Ernstfall handeln müssen – von der Kreisebene bis in die Ministerien. Ausgewählt wurden sie, weil sie eine Schnittstelle verantworten. Keine dieser Perspektiven trägt für sich.



Dr. Norbert Ahrend
Arvato Systems
Head of Public Sector Consulting



Sven Ambrosy
Friesland
Landrat



Dr. Bernd Calaminus
EnBW
Head of Business Resilience



Marlis Cremer
DRK Kreisverband Düren
Präsidentin der DRK Kreisverbände Düren und Jülich



Albrecht von Croÿ
Malteser Deutschland
Vizepräsident (bis zum 20. 6.2026)



Jens Dommel
AWS
Head of Public Sector EU & Germany



Kai Drücker
conet
CCO



Armin Fleischmann
AFCEA Bonn e.V.
Generalmajor und Vorsitzender



Prof. Dr. Hanno Friedrich
Kühne Logistics University
Associate Professor for Transport



Gerald Funke
Bundeswehr
Generalleutnant, Befehlshaber Unterstützungskommando



Dr. Christian Growitsch
HIICCE
Geschäftsführer



Wolfgang Gäbelein
DWT
Generalmajor a.D. und Vorsitzender



Dr. Timo Haas
Rheinmetall
Chief Digital Officer



Sven Hallbauer
Ewerk
Chief Revenue Officer



Thomas Hambach
Bundeswehr
Brigadegeneral, Kommandeur Landeskommando Bayern



Bernd Hellinger
soffico
Director Defence



Prof. Kai Hoberg
Kühne Logistics University
Professor für Supply Chain and Operations Strategy



Paul Höller
Land NRW
Staatssekretär



Prof. Peter Holm
BGL - Provadis Hochschule
Professor für Logistik & Supply Chain Management



Kai Hudetz
IFH KÖLN
Geschäftsführer IFH KÖLN



Prof. Dr. Christian Hummert
Cyberagentur
Forschungsdirektor und Geschäftsführer



Dr. Marianne Janik
Google Cloud
VP EMEA North, Google Cloud



Ansgar Kaltwasser
CGI
Vice President



Dr. Martha Klare
Universität der Bundeswehr München
Researcher



Prof. Dr. Wolfgang Koch
Fraunhofer FKIE
Chief Scientist



Prof. Michael Kreinest
BG Klinik Ludwigshafen
Leiter Stabsstelle Resilienz und Krisenmanagement



Peter Kuhne
IHK Bonn/Rhein-Sieg
Vizepräsident



Prof. h.c. Bernd König
Google Cloud
Managing Director



Volker Lemgen
Kreis Neuwied
Sachbearbeiter Brand- und Katastrophenschutz



Axel Lips
Sopra Steria
Associate Director Public, Defence & Security

61 Gesprächspartner, 55 geführte Interviews und zwei schriftliche Beiträge. 50 Interviews sind quantitativ ausgewertet. Drei Gesprächspartner haben einem Hintergrundgespräch zugestimmt, nicht der Nennung in der Studie. Ihre Aussagen sind ausgewertet, erscheinen aber weder in der Beteiligtenliste noch namentlich im Text Methodik im Anhang.

■ BOS ■ Staatliche Steuerung ■ Streitkräfte ■ KRITIS ■ Tech & Defense ■ Wissenschaft



Dr. Christian Marwitz
BWI
Chief Digital Officer



Benedikt Meng
infodas
Leiter Business Development & Strategie



Karsten Meywirth
Bundeskriminalamt
Director Cybercrime



Ralph Michel
secunet
Global Head of Sales Defence & Space



Dr. Christian Miller
Feuerwehr Köln
Leiter Berufsfeuerwehr



Dr. Volker Pötzsch
Bundeswehr
Generalmajor Kommando Cyber und Informationsraum



Bernd Reitmeier
Bechtle
Leitung Account Management BWL



Ansgar Rieks
AFCEA International
Generalleutnant a.D. und Vorstandsmitglied



Dr. Klaus Ritgen
Deutscher Landkreistag
Referent und Beigeordneter



Dennis Ruf
conet
Senior Vice President Sales Defense



Prof. Leif Erik Sander
Charité
Klinikdirektor, Mitglied im Expertenrat Gesundheit und Resilienz



Christian Schäfer
AWS
Head of National Security & Defense



Armin Schaus
Bundeswehr
Oberst, Operatives Führungskommando



Thomas Scholle
BDBOS
Abteilungsleiter Strategie und Steuerung



Frank Scholz
MilDef
Geschäftsführer



Tobias Schönherr
Bundespolizei
Projektleiter Digitalisierung



Dr. Rainer Sommer
Provinzial Holding
Vorstand



Dr. Christian Stufflein
Deutscher Landkreistag
Referatsleiter



Dr. Benni Thiebes
DKKV
Geschäftsführer



Thomas Tschersich
Deutsche Telekom
CSO



Felix Wang
msg systems
Senior Business Consultant Defense & Aerospace



Frank Weber
Malteser Deutschland
ZOES
COO



Sven Weizenegger
Bundeswehr
Leiter Cyber Innovation Hub



Leonard Wessendorff
Project Q
Co-Founder & CEO



Andreas Witt
Sopra Steria
Head of Cyber Security Defence & Security



Erik Zahn
Universität der Bundeswehr München
Student, Projekt Hacking4Defense



Tim Zahn
Bundeswehr
Brigadegeneral, Kommando Heer



Martin Zeidler
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Abteilungsleiter L



Dr. Hans-Martin Zimmermann
Airbus Defence and Space
Head of Engineering Defence Digital

**Liebe Leserinnen,
liebe Leser,**

Mona Neubaur
Ministerin für Wirtschaft, Industrie,
Klimaschutz und Energie

wir alle merken es in unserer dynamischen Gegenwart sehr deutlich: Sicherheit ist keine Selbstverständlichkeit. Und sie ist keine ein-dimensionale Aufgabe. Wir sprechen daher über eine umfassende Steigerung unserer Resilienz. Dies ist die Mega- und Meta-Aufgabe, die die Zeit uns stellt.

Die veränderte geopolitische Lage, hybride Bedrohungen und Cyberangriffe stellen Staat, Wirtschaft und Gesellschaft vor neue Herausforderungen und zeigen auf: Sicherheit lässt sich weder allein militärisch noch innerhalb einzelner Zuständigkeiten gewährleisten, sondern muss als gesamtgesellschaftliche Aufgabe gestaltet werden.

Die Studie „Gesamtstaatliches Sicherheitsökosystem 2030“ greift eine entscheidende Frage auf: Wie können wir vorhandene Fähigkeiten so verbinden, dass Deutschland auch unter schwierigen Bedingungen handlungsfähig bleibt? Denn leistungsfähige Institutionen, innovative Technologien und starke Unternehmen ergeben noch kein resilientes Sicherheitsgefüge. Entscheidend ist ihr Zusammenspiel – über Ressort-, Sektor- und Organisationsgrenzen hinweg.

Nordrhein-Westfalen trägt dabei besondere Verantwortung. Unser Land ist einer der bedeutendsten Industrie-, Energie- und Logistikstandorte Europas und eine zentrale Drehscheibe für Waren-, Daten- und Energieflüsse. Zahlreiche kritische Infrastrukturen, industrielle Wertschöpfungsketten und hoch spezialisierte Unternehmen sind hier beheimatet. Ihre Funktionsfähigkeit ist weit über die Landesgrenzen hinaus von Bedeutung.

Sicherheit und Verteidigungsfähigkeit beginnen deshalb nicht erst bei den Streitkräften. Sie beginnen mit sicheren Netzen, einer verlässlichen Energieversorgung, belastbaren Lieferketten und handlungsfähigen Unternehmen. Resilienz ist nicht allein eine Sicherheitsfrage, sondern zugleich ein Standort- und Wettbewerbsfaktor.



Das gilt insbesondere für kleine und mittlere Unternehmen. Sie verfügen häufig nicht über eigene Strukturen, um komplexen Cyber Risiken zu begegnen. Mit DIGITAL.SICHER.NRW unterstützt das Land Unternehmen mit praxisnahen Informationen, Veranstaltungen und neutraler Erstberatung, damit digitale Sicherheit nicht an fehlendem Wissen oder begrenzten Ressourcen scheitert.

Ebenso wichtig ist es, die unterschiedlichen Beteiligten miteinander zu vernetzen. Nordrhein-Westfalen nutzt dabei seine besondere Nähe zu Unternehmen und Kommunen, Hochschulen und Forschungseinrichtungen, Netzwerken und Verbänden, um Wissen zu bündeln und Innovationen schneller in die Anwendung zu überführen. Mit Defence.NRW stärken wir hierfür den Austausch zwischen Unternehmen, Wissenschaft und weiteren Akteurinnen und Akteuren der Sicherheits- und Verteidigungsindustrie.

Ein besonderer Ort dieser Vernetzung ist Bonn. Bundesbehörden, Bundeswehr, Wissenschaft und Wirtschaft bilden hier ein Sicherheitscluster mit nationaler Ausstrahlung. Der Bonner IT-Dialog bringt diese Perspektiven zusammen und schafft Raum für den notwendigen Austausch.

Ein resilientes Sicherheitsökosystem lebt davon, dass unterschiedliche Kompetenzen wirkungsvoll ineinandergreifen. Deshalb gilt es, vorhandene Fähigkeiten enger zu verknüpfen und bewährte Strukturen gemeinsam weiterzuentwickeln. Die Studie kann hierzu wichtige Impulse geben.

Mein Dank gilt dem AFCEA Bonn e.V. für diese Initiative und allen Beteiligten für ihre Bereitschaft, Verantwortung zu übernehmen.

Mit besten Grüßen,
Mona Neubaur

**Generalmajor
Armin Fleischmann**
Vorsitzender AFCEA Bonn e.V.



Sicherheit entsteht nicht in Silos

Obwohl es unzählige Studien, Konzeptpapiere und Arbeitsgruppen zur gesamtstaatlichen Sicherheit und Verteidigung gibt, legt AFCEA Bonn e.V. noch eine weitere vor. Warum? Weil wir die Resilienz unseres Staates erhöhen müssen. Weil uns dafür kaum Zeit bleibt. Weil eine Frage offen ist, die keine Dienststelle, Behörde oder Organisation allein beantworten kann.

Technische, rechtliche und kulturelle Defizite verstärken einander.

An vier Stellen stockt die Zusammenarbeit. Verantwortliche Stellen sind technisch nicht interoperabel. Rechtliche Schranken greifen. Organisationen arbeiten in Silos. Vertrauen und Anreize zum Informationsaustausch fehlen. Ein ressortübergreifendes Lagebild gibt es bis heute nicht. Gemeinsame Strukturen wie das Gemeinsame Terrorismusabwehrzentrum entstanden mühsam und meist als Reaktion auf konkrete Anlässe.

**Erst muss etwas passieren,
bevor sich etwas ändert.**

Wie weit uns das trägt, habe ich beim Operationsplan Deutschland gesehen. Das Operative Führungskommando der Bundeswehr hat ihn mit den Ressorts erarbeitet. Von der zivilen Seite kam daraufhin die Bemerkung, sie bräuchte ebenfalls einen General, der sich um ihren Teil kümmere. Ich habe das nie als Scherz verstanden. Der militärische Plan liegt vor. Der zivile Gegenpart fehlt, und die Bundeswehr kann ihn nicht schreiben: Dafür fehlen ihr Kenntnisse über kommunale Abhängigkeiten und Netzschaltungen.

Diese Frage kann kein Haus für sich beantworten. AFCEA Bonn e.V. führt Bundeswehr, Verwaltung, Industrie und Wissenschaft zu-

sammen, ohne für eine dieser Seiten zu sprechen. Eine Ressortstudie wird stets an den Zuständigkeitsgrenzen ihres Hauses gemessen. Wir haben 55 Tiefeninterviews geführt, von der Kreisebene bis in die Ministerien, dazu eine Online-Befragung unter 72 Technologieanbietern und Anwendern. Was in dieser Studie steht, stammt von denen, die es angeht.

Eine Studie muss sich anwenden lassen. Deshalb nennt jede Maßnahme einen Träger und eine Frist. Wir beschreiben, was das Zusammenspiel leisten soll: frühere Lageerkennung, schnellere und bessere Entscheidungen, wirksameres Handeln und längere Durchhaltefähigkeit. Wir zeigen, welche Lösungen bereits verfügbar sind, und unterscheiden zwischen fehlenden Schnittstellen und fehlenden Fähigkeiten.

Sicherheit ist kein Projekt. Sie ist eine dauerhafte staatliche Aufgabe, die im Alltag geübt und nicht im Ernstfall improvisiert wird. Was dafür zusammenwirken muss, steht auf den folgenden Seiten.

Ich wünsche Ihnen eine erkenntnisreiche Lektüre und viele Impulse, um die Silos gemeinsam aufzubrechen.

Armin Fleischmann
Vorsitzender AFCEA Bonn e.V.

Die fünf Kernbefunde

Deutschland ist nicht handlungsfähig, weil es nicht verbunden ist. Die Befunde bauen aufeinander auf: kein gemeinsames Bild, kein Mandat, kein Angebot, keine Mitwirkung – und am Ende kein Ergebnis.

K1 Die Verkettungslücke **Deutschland hat kein gemeinsames Bild der Lage**

Mittel, Fähigkeiten und Menschen sind vorhanden – die Verbindung dazwischen fehlt. 81 Prozent aller Lösungsennungen entfallen auf die beiden Enden der Kette: Lage erfassen und Wirkung erzielen. Für die Mitte, das Zusammenführen zu einem gemeinsamen Lagebild, wurden 19 von 172 Lösungen genannt, für keine ist ein Praxiseinsatz belegt. Auch die dokumentierten Lagen brechen hier: bei der Bewertung eines Signals und bei der Übersetzung einer Entscheidung in einen Auftrag.

K2 Der Systemreifegrad **Mehr als zehn Jahre Rückstand: Die Technik ist weiter als das Ökosystem**

Im Vergleich über zehn Dimensionen und sechs Länder erreicht die Bundesrepublik 14 von 30 Punkten – den niedrigsten Wert aller untersuchten Staaten und acht Punkte weniger als die Ukraine. Nur zwei der zehn Dimensionen betreffen Technik. Der Abstand liegt bei Steuerung und Durchhaltefähigkeit. Beim ressortübergreifenden Mandat hält Finnland den Standard seit dreizehn Jahren.

K3 Governance first **Es fehlt nicht die Führung, sondern ihr Mandat**

Sechs Rollen tragen das gesamtstaatliche Sicherheitsgefüge. Vier sind besetzt. Bei der verbindlichen Führung und bei der Verdichtung zum Lagebild fehlt das Mandat. Seit 2026 entstehen Strukturen: Der Nationale Sicherheitsrat tagt, ein Steuerungsstab für die zivile Verteidigung wird aufgebaut. Weisungsrecht, Rang und Personal stehen noch aus. Drei Entscheidungen schließen die Lücke. Eine neue Behörde oder eine Grundgesetzänderung ist dafür nicht erforderlich.

K4 Technologie verändert die Krise **Die Lage ändert sich schneller als die Beschaffung**

Sensorik, künstliche Intelligenz und autonome Systeme verändern Charakter und Tempo einer Krise. In drei der acht Technologie-Domänen des digitalen Rückgrats weist der erfasste Markt kein Angebot aus: Ressourcensteuerung, Wiederanlauf und Zugriffsrechte. Der Engpass entsteht auf dem Weg in die Fläche – bei Beschaffung, Integration und Skalierung.

K5 Die Bevölkerung als Ressource **Wer die Lage trägt, kommt im Angebot nicht vor**

94 Prozent der aktiven Feuerwehrangehörigen arbeiten in Freiwilligen Feuerwehren, beim Technischen Hilfswerk sind es 98 Prozent. Diese Basis trägt die Bewältigung und gleicht aus, was auf anderen Ebenen offenbleibt. 47 Prozent der Befragten benennen die Bürgereinbindung als Nachholbedarf.

Was daraus folgt

Keiner dieser Befunde verlangt eine neue Behörde, eine Grundgesetzänderung oder eine Technologie, die es noch nicht gibt. Was sie verlangen, sind Entscheidungen.

Handlungsfelder

Was bis 2030 zu tun ist

Die Untersuchung sammelte 529 Vorschläge, wie Deutschland bis 2030 handlungsfähiger wird. Verdichtet hat die Studie sie auf 30 Maßnahmen in sechs Handlungsfeldern. Jede nennt einen Träger, eine Frist und einen Nachweis. Keine verlangt eine neue Behörde, keine wartet auf Technik, die es noch nicht gibt. Je Handlungsfeld haben die Studienpartner eine Maßnahme als wichtigste gewählt. Diese sechs lassen sich sofort umsetzen.

HANDLUNGSFELD INFORMATION UND DIGITALES RÜCKGRAT Lagebilder vernetzen statt eins für alle bauen

Jede Stelle hat heute ihr Lagebild. Doch es fehlen die Verbindungen dazwischen. Wer vor Ort handelt, braucht nicht alle Informationen, sondern die richtigen. Im Fokus steht die Verbindung zwischen ziviler und militärischer Seite. Nach 24 Monaten sollen drei Ressorts und drei Länder angebunden sein. → **7.2**

HANDLUNGSFELD GOVERNANCE, RECHT UND STEUERUNG Unterhalb der großen Reform beginnen

Wer führt im Ernstfall? Wer darf handeln? Wer gibt Mittel frei? Vorrang hat die Trennung von Steuerung und Entscheidung. Der Bund definiert die Schnittstellen, die Verantwortung für die Ausführung bleibt bei Ländern, Kommunen und Betreibern. Nach 24 Monaten sollen drei Module produktiv laufen. → **7.3**

HANDLUNGSFELD RESSOURCEN, INDUSTRIE UND INNOVATION

Beschaffungstempo aus vorhandenen Verträgen holen

Material, Personal und Tempo bestimmen dieses Feld: Wie schnell kann beschafft werden, wer arbeitet im Ernstfall, was bleibt im eigenen Land herstellbar? Entscheidend ist nicht die Stückzahl im Lager, sondern die Fähigkeit, die Produktion bei Bedarf hochzufahren. Als Erstes gehören die vorhandenen Rahmenverträge geöffnet, denn dafür braucht es keine neue Ausschreibung. Nach zwölf Monaten sollen drei von ihnen behördenübergreifend nutzbar sein. → **7.4**

HANDLUNGSFELD SCHUTZ UND ABWEHR

Objektschutz und Cyberabwehr zusammendenken

Die Abwehr physischer und digitaler Angriffe bildet das kleinste Handlungsfeld und weist die schärfste Trennlinie auf. Am wichtigsten ist der Rückkanal, denn die Lagebilder gibt es bereits, nur fließt nichts zurück. Nach zwölf Monaten sollen drei weitere KRITIS-Sektoren angeschlossen sein. → **7.5**

HANDLUNGSFELD RESILIENZ UND VERSORGUNG Treffer wegstecken und wieder anlaufen

Kein Schutz hält alles ab. Was zählt, ist die Zeit bis zum Wiederanlauf. Der größte Maßnahmenblock richtet daher den Blick auf die Vorsorge. Am dringendsten ist der Wiederanlauf im Gesundheitswesen: Nach zwölf Monaten soll jede Klinik der höchsten Versorgungsstufe einen dokumentierten und einmal geübten Plan haben. → **7.6**

HANDLUNGSFELD GESELLSCHAFT, KULTUR UND ÜBEN Üben, wer im Ernstfall entscheidet

Bevölkerung, Ehrenamt, Verwaltung und politische Entscheidungsträger müssen im Ernstfall zusammenwirken. Gemeinsam mit denjenigen üben, die entscheiden, hat Priorität. Nach zwölf Monaten soll jedes Land eine ebenenübergreifende Übung mit politischer Beteiligung durchgeführt haben. → **7.7**

Jede Maßnahme hat eine Frist von zwölf oder 24 Monaten. Danach lässt sich prüfen, ob sie wirkt: Die Referenzverbindung zwischen Bundeswehr und ziviler Seite läuft, oder sie läuft nicht. Der Wiederanlaufplan ist geübt, oder er ist es nicht. Kapitel 7 führt alle 30 Maßnahmen aus, Abschnitt 7.8 nennt die Zielmarke für 2030. Was sie verlangen, sind Entscheidungen. → **7.8**

01

Gesamtstaatliche Sicherheit

**Zeit wird
zur kritischen
Variable**

1.0 – DER BEFUND

Drei von vier sehen Deutschland nicht handlungsfähig



Eine Drohne kann in 30 Sekunden mehrere Zuständigkeitsräume berühren. Deutschland braucht oft länger, um aus Erkennen gemeinsames Handeln zu machen. Der Handlungsfähigkeits-Index von 36 Punkten misst diesen Abstand.

Die neue Lagerealität bewegt sich schneller als die Ordnung, die sie bearbeiten soll. Drohnen wechseln Zuständigkeitsräume, Stromausfälle ziehen Kommunikation und Versorgung mit, und bei hybriden Angriffen bleibt die Ursache zunächst offen. Aus einer fachlich beherrschbaren Lage wird binnen Minuten eine ressortübergreifende Lage. → [1.1](#)

Was Verfahren offenlassen, fangen Menschen auf. Rund 1,76 Millionen Engagierte im Bevölkerungsschutz, persönliche Kontakte und improvisierte Entscheidungen halten Lagen handhabbar und verdecken zugleich, welche Struktur beim nächsten Ereignis erneut fehlen wird. Improvisationsfähigkeit wird damit zur Messlatte für die Belastbarkeit des Systems. → [1.2](#)

Die Verkettungslücke hat eine technische und eine organisatorische Bauform. Das ‚Spaghetti-Interface‘ von Bernd Hellinger, soffico, beschreibt Punkt-zu-Punkt-Verbindungen, die mit jedem neuen System unübersichtlicher werden. 81 Prozent der codierten Wirkungsbezeichnungen liegen an den Enden der Kette, Erkennen und Handeln. Die verbindende Mitte aus Bewertung, Entscheidung und Koordination bleibt dünn. → [1.3](#)

Drei Handlungsketten machen diesen Befund überprüfbar: Warnen, Lagebild und Wirken. In allen drei Fällen funktioniert der erste technische Schritt, Zeit geht bei der Übergabe an die nächste Stelle verloren. Jede Kette lässt sich bis zu ihrer eigenen Bruchstelle verfolgen. → [1.4](#)

Am Ende steht eine klare Diagnose. Fähigkeiten, Recht, Technik und Personal sind in weiten Teilen vorhanden. Ihre Wirkung hängt von vorab geklärten Übergaben, Mandaten und gemeinsamer Übung ab. Zuständigkeit ist geregelt – überprüfbare Verantwortung für das Ergebnis ist es nicht. → [1.5](#)

1.1 – DIE NEUE LAGEREALITÄT

Lagen halten sich nicht an Ressortgrenzen

Über einem sicherheitsrelevanten Werksgelände in Bremen kreisen regelmäßig Flächendrohnen mit Kameras. Sie fliegen unterhalb der Radarschwelle der Flugsicherung. Der Betreiber hat eine Dachkamera und ein passives Ortungsgerät für Funksignale installiert. Er erkennt Drohne und mutmaßlichen Pilotenstandort. Eingreifen darf er nicht. Bis die Polizei eintrifft, ist das Fluggerät verschwunden.

Timo Haas von Rheinmetall verortet das Problem nach der Erkennung. Betreiber, Landespolizei, Bundespolizei, Flugsicherung und Bundeswehr verfügen über unterschiedliche Informationen und Befugnisse. Keine Stelle kann allein klären, ob eine Spielerei, Werksspionage oder staatliche Aufklärung vorliegt. Diese Bewertung bestimmt jedoch, wer handeln darf. Während die Beteiligten Informationen und Zuständigkeiten abgleichen, läuft die verfügbare Zeit ab.

Damit wird die Zuständigkeitsfrage Teil der Lage. Die staatlichen Strukturen stammen aus einer Ordnung, in der Ereignisse meist einem Sektor zugeordnet werden konnten. Bei komplexen Lagen reicht diese Voraussetzung nicht mehr.

Vier Entwicklungen verschärfen das Problem. Was über dem Bremer Werksgelände als wiederkehrender Vorgang sichtbar wird, kann andernorts in einer halben Minute mehrere Zuständigkeitsräume berühren. Axel Lips von Sopra Steria beschreibt den Zeitdruck: „Fliegt eine Drohne zwischen Bundeswehrliegenschaft, Autobahn und Gefängnis hin und her, berührt sie in 30 Sekunden drei, vier Zuständigkeitsbereiche.“

Erstens überlagern sich Lagen. Eine Hitzeperiode belastet das Stromnetz, während eine Cyberkampagne läuft und Desinformation die Warnkommunikation stört. Jede zuständige Stelle bearbeitet ihren Ausschnitt. Ohne gemeinsame Bewertung bleibt unbemerkt, dass die Ereignisse einander verstärken.

Zweitens überschreiten Ausfälle Systemgrenzen. Fehlender Strom beeinträchtigt Kommunikation, Verwaltung und Versorgung. Diese Abhängigkeiten sind bekannt, aber nicht vollständig erfasst. Die Vorsorge einzelner Netze reicht nicht aus, sobald mehrere Infrastrukturen nacheinander ausfallen.

Drittens kann ein Unfall anfangs wie ein Angriff wirken. Bei einem ausgefallenen Umspannwerk, einer kompromittierten Kommunalverwaltung oder einer gestörten Lieferverbindung ist die Ursache zunächst offen. Zivile Gefahrenabwehr und Verteidigung können ihre Reaktion daher nicht von einer schnellen Zuordnung des Urhebers abhängig machen.

Viertens bestimmt ein Angreifer den Zeitpunkt. Er kann gezielt jene Minuten nutzen, in denen Behörden Informationen austauschen und Befugnisse klären. Zeit ist damit zur entscheidenden Systemvariable geworden. Drohnenschwärme über kritischen Infrastrukturen, KI-gestützte Cyberangriffe und Sabotage an Verkehrs- oder Energienetzen verkürzen die Entscheidungszeit.



„Russland orientiert sich an dem, was wir militärisch auch täten: Man greift am besten die Schnittstellen an, die Zuständigkeitsgrenzen.“

Thomas Hambach • Brigadegeneral, Landeskommandeur Bayern, Bundeswehr

Eine Lage ist in dem Moment keine Ressortaufgabe mehr, in dem ihre Bewertung Informationen erfordert, über die keine zuständige Stelle allein verfügt.

Unfall, Angriff, Sabotage: Die Folgen überschreiten Zuständigkeiten

Drei Ereignisse zeigen die Reichweite solcher Abhängigkeiten. Die Sprengung der Nord-Stream-Leitungen im Jahr 2022 beeinflusste Energiepreise und Versorgungsplanung. Eine abschließende internationale Zuordnung fehlt. Der Ausfall eines Netzknotens in Berlin-Adlershof wirkte 2024 auf Verkehr, Kommunikation und Verwaltung zugleich. Der Cyberangriff auf Anhalt-Bitterfeld zwang die Kreisverwaltung 2021 für sieben Monate in den Notbetrieb und verursachte einen Schaden von 2,5 Millionen Euro. In jedem Fall überschreitet eine Störung binnen Stunden die Grenzen des Sektors, in dem sie entstand.

Der Gesetzgeber hat darauf reagiert. Das Dachgesetz zur Stärkung der physischen Resilienz Kritischer Infrastrukturen (KRITIS-Dachgesetz) trat am 17. März 2026 in Kraft. Es setzt bundeseinheitliche und sektorübergreifende Mindestanforderungen für kritische Anlagen. Der Schutz richtet sich nach den Folgen eines Ausfalls, nicht nach dessen Ursache. Offen bleibt, welche Stelle sektorale Meldungen zu einer verbindlichen Gesamtlage zusammenführt (Bundesministerium des Innern, BMI, 2026).

Innen-, Verteidigungs- und Verkehrsressort arbeiten in diesem Fall mit getrennten Lageausschnitten. Das Verteidigungsressort beschafft für militärische Aufgaben. Das Innenressort verweist bei hybriden Bedrohungen auf rechtliche und technische Grenzen. Unternehmen investieren deshalb in eigene Sensorik und prüfen passive Abfangsysteme. Der Staat muss festlegen, welche Schutzleistung Betreiber erbringen dürfen und ab welchem Punkt eine befugte Behörde übernimmt.

Der Kipppunkt liegt dort, wo die Bewertung Informationen aus mehreren Zuständigkeiten verlangt. Fünf Stellen sehen die Drohne, keine darf sie allein bewerten. Bis die Zuständigkeit geklärt ist, ist sie weg. Daran ändert auch das Gemeinsame Drohnenabwehrzentrum nichts.

Seit Dezember 2025 arbeitet bei der Bundespolizei das Gemeinsame Drohnenabwehrzentrum von Bund und Ländern. Es soll Informationen bündeln und ein nationales Lagebild fördern (BMI, 2025). Thomas Hambach vom Landeskommmando Bayern grenzt den Auftrag ein: Das Zentrum koordiniert vor allem die Entwicklung von Fähigkeiten, einzelne Einsätze steuert es nicht. Damit verbessert es den Austausch, schafft jedoch noch kein Mandat für eine verbindliche Entscheidung am konkreten Ort.

Ressortgrenzen sichern Haftung, Finanzierung und demokratische Kontrolle. In komplexen Lagen benötigen sie einen verbindlichen Übergang zur gemeinsamen Bewertung. Fehlt er, vergeht Zeit, obwohl Fachleute und Daten bereitstehen. Der offene Punkt lautet:

Wer bewertet die Gesamtlage, wer darf daraus einen Auftrag ableiten, und für wen ist diese Bewertung verbindlich? Die operative Ebene trägt die Folgen dieser Verzögerung.

KIPPPUNKT

Kein Akteur ist für das Ganze zuständig

RESSORTLAGE

GESAMTSTAATSLAGE

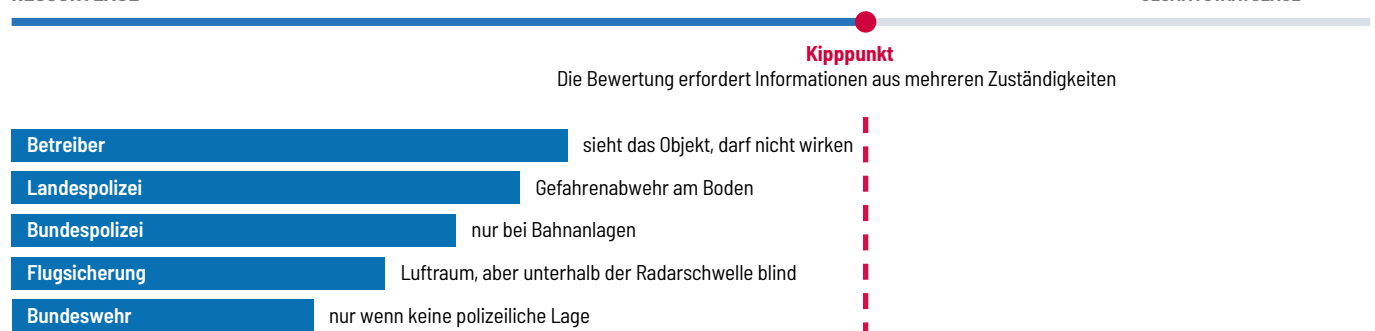


Abb. 1.2: Tiefeninterview Rheinmetall, Zielbild GSÖ 2030

1.2 – KOMPENSATION DURCH IMPROVISATION

Die Einsatzkräfte tragen, was oben nicht entschieden wird



Behörden und Organisationen mit Sicherheitsaufgaben gleichen strukturelle Defizite im Einsatz aus. Sie improvisieren, weil Lagebilder getrennt bleiben, Übergaben nicht eingeübt sind oder ein klares Führungsmandat fehlt. Diese Leistung ist unverzichtbar. Sie darf jedoch nicht als Beleg für eine belastbare Struktur missverstanden werden.

FALLBEISPIEL • KREIS NEUWIED, JULI 2021

Von der Flutnacht am Mittwoch, 14. Juli 2021, bis zum Samstag arbeitete der Kreis Neuwied rund vierzig Stunden ohne zentrale Einsatzleitung. Die überörtliche Bereitschaft war aktiviert, die Einsatzabschnitte organisierten sich in der Fläche, Menschen trafen Entscheidungen und verschoben Ressourcen. Erst am Samstag nahm die zentrale Einsatzleitung ihre Arbeit auf. Volker Lemgen, der die Lage vor Ort verantwortete, nennt diesen Zeitraum die „verlängerte Chaosphase“.

Drei Befunde zeigen, warum: Die Koordination bleibt unten hängen, das Versäumnis wird nicht sichtbar, und die Basis ist freiwillig.

Erstens bleibt die Koordination an den Einsatzkräften hängen.

Feuerwehren löschen, Rettungsdienste versorgen, Stäbe planen. Zusätzliche Belastung entsteht bei ungeklärter Führung, widersprüchlichen Lagebildern und konkurrierenden Anforderungen an dieselbe Ressource.

„Wir haben mehrere Hüte auf, aber wenn es drauf ankommt, können wir nur an einer Stelle arbeiten.“

Michael Kreinest • Leiter Stabsstelle Resilienz und Krisenmanagement, BG Klinik Ludwigshafen

Zweitens löscht erfolgreiche Improvisation ihre eigene Spur. Jede Lücke verschwindet in dem Moment, in dem sie geschlossen wird. Dann gilt ein Einsatz als bewältigt, obwohl persönliche Kontakte, freiwillige Arbeit oder zufällig verfügbare Geräte den Ausschlag gaben.

Drittens gibt es ohne Ehrenamt keinen Bevölkerungsschutz. Rund 94 Prozent der aktiven Feuerwehrangehörigen arbeiten in Freiwilligen Feuerwehren, beim THW sind etwa 98 Prozent ehrenamtlich tätig. Insgesamt engagieren sich rund 1,76 Millionen Menschen im Bevölkerungsschutz (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK, 2026). Wer davon im Ernstfall kommt, weiß niemand.

„Wenn das Ehrenamt wegfällt, können Sie den Laden sofort zumachen.“

Albrecht von Croÿ • Vizepräsident, Malteser Hilfsdienst

Niemand hält Deutschland für voll handlungsfähig – auch die nicht, die es tragen

Sie wissen, warum. Behelfe füllen die Lücken der Sicherheitsarchitektur: Kostenanreize entscheiden, wer gerufen wird. Persönliche Kontakte ersetzen den Verwaltungsweg. Und dieselben Menschen sind militärisch und zivil verplant. Im Bündnisfall trägt das nicht mehr.

Wer nichts kostet, wird gerufen. In der ersten Welle der Pandemie baten Landräte und Bürgermeister häufig die Bundeswehr um Hilfe beim Betrieb von Alten- und Pflegeheimen. Ausschlaggebend war nach den Interviews dieser Studie nicht allein die verfügbare Leistung. Amtshilfe der Streitkräfte belastete die Kommune finanziell anders als der Einsatz eines Hilfswerks. Diese Anreize beeinflussen, welche Ressource angefordert und in künftigen Plänen erneut vorgesehen wird.



„Der Oberstleutnant schickt keine Rechnung.“

Albrecht von Croÿ • Vizepräsident
Malteser Hilfsdienst

Wer sich kennt, bekommt Hilfe. In der akuten Lage ersetzen persönliche Kontakte häufig den vorgesehenen Verwaltungsweg. Die Hilfe erreicht ihren Einsatzort, Abrechnung und Zuständigkeit werden später geklärt. Ein belastbares Verfahren darf jedoch nicht davon abhängen, ob die Verantwortlichen einander bereits kennen.

Im Bündnisfall trägt diese Basis nicht mehr. Die Bundeswehr kommt dann nicht zur Unterstützung, sondern wird selbst gebraucht, Abschnitt 4.6 führt das aus. Die Belastung beginnt früher – eine Bindung

an der Ostflanke wirkt im Inland, auch ohne förmlich festgestellten Verteidigungsfall. Gleichzeitig fallen Reservisten an ihren zivilen Arbeitsplätzen aus. Bei der Cyberagentur ist ein zweistelliger Prozentsatz der Beschäftigten zugleich Reservist. Solche Doppelverplanungen schwächen militärische und zivile Strukturen zur selben Zeit.

Niemand darf zählen, wer doppelt verplant ist. Rainer Sommer von der Provinzial müsste wissen, welche seiner Mitarbeitenden ehrenamtlich bei Feuerwehr oder THW gebunden sind, um sich auf den Spannungsfall vorzubereiten. Genau diese Daten darf er aus Arbeitsschutzgründen nicht erheben. Vierzehn Gesprächspartner benennen die Mehrfachverplanung unabhängig voneinander – eine belastbare Zahl gibt es nicht.

36 von 100 Punkten. Die Befragung dieser Studie hat 72 Anbieter und Anwender nach der Handlungsfähigkeit Deutschlands in komplexen Lagen gefragt. 61 Prozent halten das Land für eingeschränkt handlungsfähig, 15 Prozent für nicht handlungsfähig. Niemand hält es für vollständig handlungsfähig. Der Handlungsfähigkeits-Index fasst das zu 36 von 100 Punkten zusammen.

Die operative Ebene hält das System an Stellen zusammen, für die kein Verfahren vorgesehen ist. In der Krise funktioniert es – weil Rahmenbedingungen und Vorgaben temporär beiseitegeschoben werden. Genau diese Entscheidungen fehlen vorher. Was dort ausgeglichen wird, ist kein Ausführungsproblem, sondern ein Konstruktionsfehler in der Sicherheitsarchitektur.

SELBSTBEFUND

Kein Befragter hält Deutschland für voll handlungsfähig



GEGENPROBE – URTEIL NACH BEFRAGTENGROUPE

Anbieter		rund zwei Drittel der Stichprobe
Anwender		Bedarfsträger und Betreiber
Forschung		Wissenschaft und Institute
Führungsebene		urteilt am strengsten

Die Anbieterseite hätte Anlass, das System günstiger darzustellen. Ihr Urteil weicht kaum ab – das Ergebnis ist unabhängig vom Interesse der Befragten.

N = 72 · Feldschluss Juni 2026 · Index $(0-1)/3 \times 100 = 36$ von 100

Abb. 1.3: GSÖ-Befragung

1.3 – DIE VERKETTUNGSLÜCKE

Nicht die Fähigkeit fehlt, sondern die Orchestrierung

Deutschland hat kein Erkenntnisproblem und in der Breite kein Technologieproblem. Es hat ein Problem in der Sicherheitsarchitektur. Die Interviews unterscheiden drei Lücken: eine Orchestrierungslücke, eine Mandatslücke und eine Fähigkeitslücke.



„Unser Hauptproblem sind nicht fehlende Technologien oder Fähigkeiten, das Hauptproblem ist fehlende Orchestrierung.“

Prof. Dr. Christian Hummert • Forschungsdirektor und Geschäftsführer, Cyberagentur

Die Orchestrierungslücke trennt Systeme, die einzeln funktionieren.

Bund, Länder, Bundeswehr und Betreiber entwickeln eigene digitale Lagebilder und Einsatzsysteme. Mehrere Vorhaben funktionieren innerhalb ihres jeweiligen Bereichs. Eine bundesweit verbindliche Verbindung dieser Systeme fehlt. Die Länder- und Ressortübergreifende Krisenmanagementübung (LÜKEX) weist seit 2004 wiederholt Führungsbrüche an solchen Übergängen nach. Der Durchgang 2023 bestätigte den Übungsbedarf.

Was stattdessen entsteht, hat einen Namen.

„Wir nennen das immer gern das Spaghetti-Interface – jedes System spricht vier, fünf andere an.“

Bernd Hellinger • Director Defence, soffico

Jedes System baut eigene Verbindungen zu vier, fünf anderen auf.

Mit jedem neuen System wächst die Zahl der Verbindungen schneller als die Zahl der Systeme. Was als Effizienzgewinn beginnt, endet als Geflecht, das niemand mehr überblickt – und das bei jedem Ausfall an einer anderen Stelle reißt.

Es reißt an den Übergängen. Ein Signal muss bewertet, in ein gemeinsames Lagebild eingeordnet, in einen Auftrag übersetzt und nach dem Einsatz in einen geordneten Wiederanlauf überführt werden. Bei jedem Schritt können Zuständigkeit, Datenformat und Führungsregel wechseln. Fehlt ein Verantwortlicher für die Übergabe, bleibt ein funktionierendes Einzelsystem ohne Wirkung auf die Gesamtlage.

Die Mandatslücke lässt zwei Übergänge ohne Träger. Der erste liegt zwischen Datensammlung und verbindlicher Bewertung. Der zweite verbindet Koordination über Ebenen hinweg mit der Befugnis zur Führung. Timo Haas von Rheinmetall nennt verfügbare Quellen: Telemetrie aus Mobilfunknetzen, öffentliche Videoströme und Senso-

ren von Betreibern kritischer Infrastrukturen. Datenschutz, Einstufungen und getrennte Ressortverfahren begrenzen ihre gemeinsame Auswertung.

Die Fähigkeitslücke betrifft vier Bereiche. Bei souveräner satellitengestützter Aufklärung, priorisierbarer Satellitenkommunikation, der Abwehr unbemannter Systeme und analogen Rückfallebenen fehlen teilweise eigene Fähigkeiten. Hinzu kommen Abhängigkeiten von Anbietern, deren Leistungen der Staat im Krisenfall nicht priorisieren kann. Benedikt Meng von infodas erwartet im Bündnisfall frühe Ausfälle bei der Satellitenkommunikation. Martin Zeidler vom BBK verweist auf fehlende analoge Rückfallverfahren.

Orchestrierung verlangt Standards, Mandate verlangen klare Befugnisse und Fähigkeiten verlangen langfristigen Aufbau und regelmäßige Erprobung.

Der Lösungsbestand zeigt dieselbe Schieflage. Von 48 primär codierten Wirkungsnennungen entfallen 81 Prozent auf die beiden Enden der Kette: Erkennen und Handeln. Bewerten, Entscheiden und Koordinieren bleiben deutlich dünner besetzt, Orchestrierung erhält eine einzige Wirkungsnennung.

19

von 172 Lösungen

haben überhaupt einen Orchestrierungsbezug. Keine einzige ist durch einen Praxisbeleg gedeckt. Zugleich erreicht Führung die höchste Bewertung aller Reifedimensionen im erfassten Bestand. Die Reife bezieht sich auf einzelne Führungssysteme, nicht auf ihr Zusammenwirken. Genau dort entsteht die Lücke.

Lösungs-Datenbank GSÖ 2030, Stand Juli 2026 · 131 Nennungen aus Interviews und 41 Einträge aus der Befragung

Zivil und militärisch planen beide sorgfältig aneinander vorbei

Zwei Pläne rechnen mit denselben Lagern. Ein Lebensmitteleinzelhändler erfuhr, dass seine Bestände in der militärischen Operationsplanung für die Versorgung eingeplant sind. Der zivilen Vorratsplanung, die mit denselben Lagern rechnet, fehlte diese Information. Hanno Friedrich von der Kühne Logistics University beschreibt den Fall als Folge parallelen Planens: zwei sorgfältige Pläne, dieselbe Ressource, kein gemeinsames Wissen.

Im Gesundheitswesen gibt es keine Stelle, die verteilen darf. Leif Erik Sander von der Charité fragt: „Wen soll das Militär im zivilen Gesundheitswesen anrufen? Das gibt es gar nicht.“ Soldaten folgen zunächst der sanitätsdienstlichen Kette bis zu den Bundeswehrkrankenhäusern. Deren rund 1.800 Betten reichen bei einer Planannahme von bis zu 1.000 Verwundeten täglich nur kurze Zeit. Dann braucht die Bundeswehr zivile Kliniken. Dort verteilen sich Verantwortung und Kapazitätsplanung auf Länder, Kommunen, Leitstellen und Träger. Eine bundesweit handlungsbefugte Patientensteuerung fehlt.

Und umgekehrt hängt die militärische Seite an ziviler Infrastruktur. Seit dem russischen Großangriff auf die Ukraine richtet sich die Bundeswehr mit hoher Intensität auf Landes- und Bündnisver-

teidigung aus. Christian Marwitz vermisst eine vergleichbare Anstrengung im zivilen Teil der Gesamtverteidigung. Militärische Führung hängt von Stromnetzen, Funkmasten, Rechenzentren, Transportwegen und Treibstoff ab. Fallen diese Leistungen aus, verlieren Einsatzpläne und Informationstechnik ihre Grundlage. Zuständigkeiten sind vielfach geregelt. Ungeklärt bleibt, wer die benötigten zivilen Infrastrukturen unter den Bedingungen eines großflächigen Angriffs verfügbar hält.



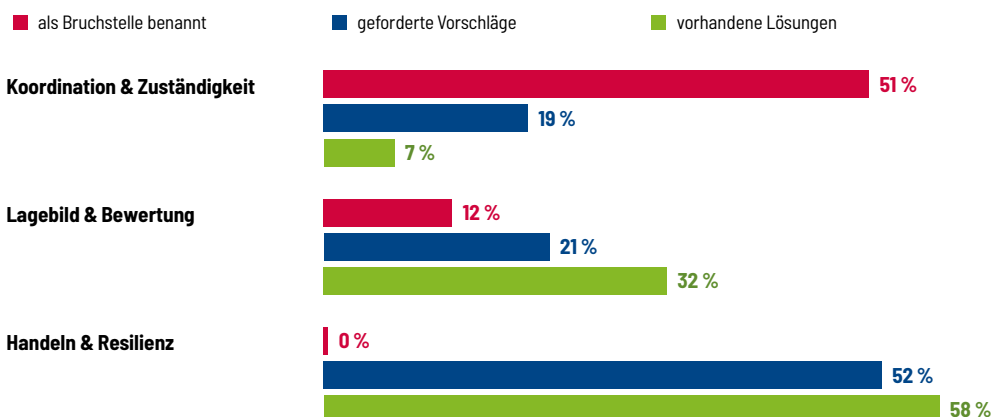
„Die Führungsfähigkeit in der Krise läuft ins Leere, wenn sie sich auf eine Kommunikationsinfrastruktur mit Funkmasten abstützt, deren Stromversorgung großflächig ausgefallen ist.“

Dr. Christian Marwitz • Chief Digital Officer, BWI

Was die drei Fälle zeigen, bestätigt die Befragung. Die Hälfte der Gesprächspartner verortet den Bruch bei Koordination und Zuständigkeit – er ist bei Technologieanbietern wie bei Anwendern bekannt. Bedient wird er nicht: Dorthin zielen 19 Prozent der Vorschläge und 7 Prozent der Lösungen. Beim Handeln ist es umgekehrt. Dort sieht fast niemand einen Bruch, und dort liegt das meiste Angebot.

BRUCHSTELLEN

Verbindung zwischen Koordination und Zuständigkeiten selten bedient



Grundlage: 49 Nennungen · 529 Vorschläge · 172 Lösungen

Abb. 1.4: Auswertungsraster 3.1 – und Lösungs-Datenbank GSÖ 2030

1.4 – DIE BRUCHSTELLEN

Lagebild, Warnen, Wirken: drei Ketten, die immer wieder reißen

Die Technik funktioniert in allen drei Ketten: Sensoren liefern Daten, Warnkanäle erreichen Geräte, Wirkmittel existieren. Was danach kommt, ist nicht geregelt – wer bewertet, wer warnt, wer wirken darf und womit.

Das Lagebild gehört niemandem. Auf die Frage, wie weit das Bundesamt auf dem Weg zu einem gemeinsamen Lagebild sei, antwortet Martin Zeidler vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): vielleicht 30 bis 40 Prozent. Deutschland besitzt ein nationales Lagezentrum und 16 Landeslagezentren, aber kein dauerhaftes gemeinsames Lagezentrum.

Institutionell ist der Weg beschrieben: Über das Gemeinsame Melde- und Lagezentrum (GMLZ) erstellt das BBK die Fachlage Bevölkerungsschutz. Sie fließt mit polizeilicher und nachrichtendienstlicher Lage in die innere Lage, mit der militärischen Lage zur zivilen Gesamtlage und künftig im Nationalen Sicherheitsrat zusammen. Praktisch beruht die Weitergabe von Lageinformationen jedoch wesentlich auf Absprachen und Freiwilligkeit: auf der Bereitschaft einzelner Personen, in einer akuten Lage Informationen weiterzugeben, deren Nutzen sie für sich selbst gerade nicht erkennen. So entstehen mehrere Lagebilder, ohne dass eine Stelle verbindlich festlegt, welches Gesamtbild für die Entscheidung gilt.

Beim Warnen reißt es zweimal. Eine versandte Warnung braucht eine kleinräumige Bewertung, die Menschen in Handlung übersetzen können. In der Flutnacht bezogen sich Wetterhinweise in der Städteregion Aachen auf einen Raum von Baesweiler bis in die Eifel. Für eine konkrete Warnentscheidung war diese Auflösung zu grob. Marlis Cremer von den DRK-Kreisverbänden Düren und Jülich beschreibt die Folge: Ohne genaue Lage lässt sich keine belastbare Warnung formulieren.

Und ein zweites Mal nach der Zustellung. Seit Februar 2023 erreicht das Mobilfunk-Warnsystem Cell Broadcast jedes eingeschaltete Mobiltelefon in einer Funkzelle, ohne Anwendung, Anmeldung oder zusätzliche Netzlast. Zustellung allein löst jedoch keine Schutzhandlung aus. Im Ahrtal lagen Warnungen vor. Evakuierungsaufträge folgten nicht rechtzeitig. Beim bundesweiten Warntag 2023 blieb zudem unbekannt, wie die Bevölkerung reagierte, weil ein Rückkanal fehlt.

Beim Wirken ist die Befugnis geklärt, das Mittel nicht. Bei der Abwehr unbemannter Systeme verteilen sich Befugnisse auf Bundespolizei, Landespolizeien, Flugsicherung und Bundeswehr. Das

Gemeinsame Drohnenabwehrzentrum verbessert den Austausch. Im Einzelfall fehlt weiterhin ein gemeinsames Luftlagebild. Mehrere befugte Stellen gewinnen keine Handlungszeit, solange sie dasselbe Objekt nicht gleichzeitig sehen und bewerten können.

Neun Gesprächspartner beschreiben diese Verzögerung. Leonard Wessendorff von Project Q berichtet aus dem Reallabor am früheren Flughafen Tegel: Eine Drohne lässt sich erkennen, nach dem Anruf bei der Polizei ist die Lage meist beendet. Paul Höller aus dem nordrhein-westfälischen Wirtschaftsministerium verweist auf zentral organisierte Abwehrkräfte in Nordrhein-Westfalen, die vor allem Großereignisse absichern. Thomas Tschersich von der Deutschen Telekom beschreibt das Problem aus Sicht eines Rechenzentrums: Eine Polizei, die erst nach dem Abflug eintrifft, kann die Anlage nicht schützen.

Anfang 2026 hat der Gesetzgeber nachgezogen: Die Novelle des Luftsicherheitsgesetzes erlaubt den Streitkräften nach Paragraph 15a als letztes Mittel Waffengewalt gegen unbemannte Fluggeräte. Für ein ganzes Bundesland stehen zwei Drohnenabwehrzüge bereit.



„Die rechtlichen Rahmenbedingungen, schon bei Annäherung einer Drohne an eine militärische Anlage, sind geklärt. Jetzt müssen die entsprechenden Wirkmittel in die Fläche gebracht werden und interne Anweisungen angepasst werden.“

Tim Zahn • Brigadegeneral, Kommando Heer, Bundeswehr

Alle drei Ketten hängen an derselben Leitung

Timo Haas von Rheinmetall berichtet, dass Einsatzkräfte bei Flutkatas-trophen auf zivile Mobilfunknetze und kommerzielle Nachrichten-dienste ausweichen. Analoges Funk, behördlicher Digitalfunk und taktische Systeme der Bundeswehr arbeiten nicht durchgehend zusammen. Die technische Schnittstelle wurde jahrelang verzögert. Am Einsatzort bleiben deshalb mehrere Funkgeräte und getrennte Gesprächskreise.

50

Kilobit pro Sekunde

Für 20 Teilnehmer – die realen Datenraten im taktischen Funk der Bundeswehr. Eine Größenordnung aus der Zeit vor ISDN. Wer Lagebilder teilen will, teilt sie über diese Leitung.

Tiefeninterview : Timo Haas, CDO, Rheinmetall

Der Zielzustand ist amtlich beschrieben. Zivile Lageinformationen von Bund und Ländern sollen zu einem bewerteten Lagebild Inland zusammenlaufen. Dieses soll mit dem militärischen Lagebild und dem Lagebild Ausland verbunden werden (Innenministerkonferenz, IMK, 2025). Bislang beschreibt der Text eine Absicht, keinen erreichten Zustand.

Für den schwersten Fall ist niemand zuständig. Für das Szenario mit dem größten Kaskadenpotenzial hält das BBK fest, dass keine Be-hörde mit der Notfallplanung für Stromausfälle befasst ist. Bund, Länder, Kommunen und Betreiber handeln in eigener Zuständigkeit (BBK, 2026).

Auch der Markt zeigt den Engpass. Die Befragung hat Anbieter gefragt, welche Wirkung ihre Lösungen versprechen, und die Inter-views, welche Wirkung gefordert wird. Beide Seiten nennen dieselben drei Stufen: früher erkennen, besser entscheiden, wirksamer handeln. Beim Erkennen und beim Handeln bietet der Markt mehr an, als gefordert wird. Bei den Entscheidungen fallen beide Werte auf den kleinsten Stand: 8,5 Prozent der Lösungen versprechen hier Wirkung, 12,9 Prozent der geforderten Vorschläge zielen darauf. Interviews und Marktdaten weisen damit auf dieselbe Stelle.

Die Bruchstellen verlangen unterschiedliche Korrekturen: ein verbindliches gemeinsames Lagebild, verständliche Warnungen mit Rückkanal und Wirkmittel dort, wo die Befugnis bereits gilt. Zusätz-liche Technik hilft erst, sobald Zuständigkeit, Übergabe und Übung geregelt sind.

MARKTLÜCKE

Der Markt liefert kaum Lösungen

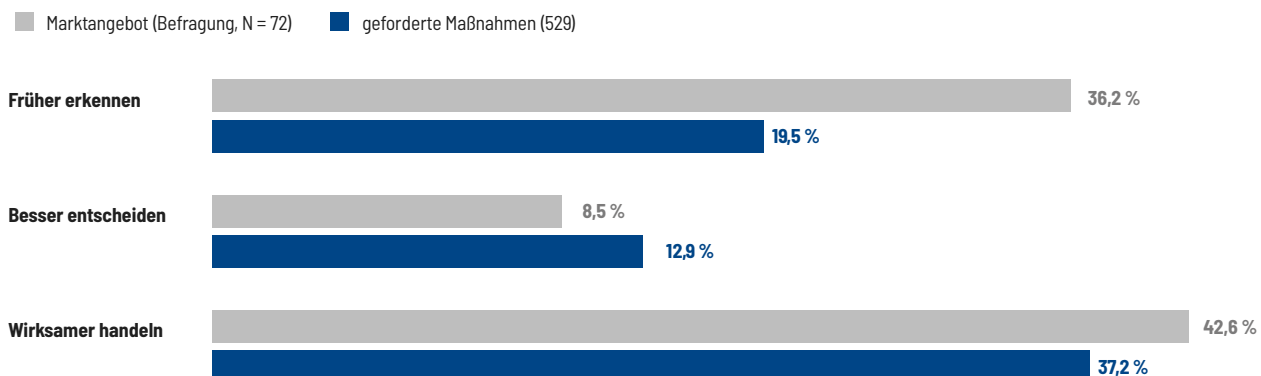


Abb. 1.5: GSÖ-Befragung, Maßnahmen-Datenbank GSÖ 2030

1.5 – DIE KONSEQUENZ

Zuständigkeit organisiert keine Wirkung

Die Interviews zeigen, dass vorhandene Fähigkeiten im Ernstfall ungenutzt bleiben, solange Befugnisse, Verantwortung und Haftung nicht vorab geklärt sind. Die Befunde benennen damit die Bedingungen der Handlungsfähigkeit. Die notwendigen Maßnahmen folgen in Kapitel 7.



„Dann wird gefragt: Wer darf was?
Anstatt: Wer kann was tun?“

Prof. h.c. Bernd König • Managing Director,
Google Cloud

Die Frage wird falsch herum gestellt. Bernd König von Google Cloud kritisiert eine institutionelle Reflexbewegung. Die Frage nach vorhandenen Fähigkeiten darf nicht hinter Ressortgrenzen verschwinden. Daraus folgt kein Vorrang des Handelns vor dem Recht.

Die richtige Reihenfolge ist entscheidend. Der Staat muss vor der Krise klären, welche Organisation über welche Technik, welches Personal und welche Erfahrung verfügt. Anschließend sind Befugnisse, Verantwortung und Haftung so zu ordnen, dass diese Fähigkeiten im Ernstfall ohne langwierige Zuständigkeitsdebatte eingesetzt werden können.

Die Strukturen sind da, ihnen fehlt der gemeinsame Auftrag. Martin Zeidler fordert ein Mandat für das BBK. Tobias Schönherr von der Bundespolizei hält ebenfalls keinen neuen Apparat für nötig. Benedikt Meng von infodas verweist auf das Militär, wo Multidomain längst heißt, dass Zuständigkeiten entlang von Wirkungszielen gedacht werden. Bernd König ergänzt die praktische Voraussetzung: „Üben, üben, üben.“ Ressort-, ebenen- und sektorübergreifende Szenarien müssen mit allen beteiligten Stellen trainiert werden.

Wer orchestrieren könnte, hat kein Mandat. Wer eines hätte, weiß nicht, dass er es hat. Nach Übungen und Einsätzen braucht es deshalb eine verbindliche Rückschau. Sie muss erfassen, welche improvisierten Leistungen den Erfolg ermöglichten, welche Ressourcen mehrfach eingeplant waren und welche Entscheidungen zu spät fielen.



„Wir müssen das personalisierte Netzwerk zu
einem institutionalisierten Netzwerk machen.“

Thomas Hambach • Brigadegeneral, Landes-
kommandeur Bayern, Bundeswehr

Der Rechtsrahmen ist nicht der einzige Engpass. Von 101 Lösungen mit bestimmbar Hemmnissen nennen sieben eine rechtliche Hürde, Steuerung und Beschaffung erreichen jeweils 27 Nennungen. Die geringere Zahl rechtlicher Nennungen beweist nicht, dass alle Befugnisse genügen. Vollzugsdefizite, widersprüchliche Vorgaben und ungeeignete Verfahren können Wirkung verhindern. Benötigt werden vorab geklärte Mandate und ein Recht, das ihren Einsatz ermöglicht.

Nicht jedes Risiko lässt sich versichern. Rainer Sommer von der Provinzial verweist darauf, dass Krieg und Kriegsfolgen weltweit von der Deckung ausgeschlossen sind. Rückversicherer bieten das kaum kalkulierbare Risiko nicht an. Auch bei Cyberangriffen verschiebt sich die Grenze der Versicherbarkeit. Wo private Deckung endet, muss staatliche Vorsorge festlegen, welche Leistungen verfügbar sein müssen und wer ihre Finanzierung trägt.

Die dokumentierten Fälle zeigen die Folgen unterlassener Vorbereitung. Handlungsfähigkeit entsteht vor der Krise: durch verbundene Informationen, rechtzeitig geklärte Mandate, verfügbare Fähigkeiten und gemeinsame Übung. Im Einsatz entscheidet dann nicht die Improvisation allein, wie lange der Staat bis zur wirksamen Handlung braucht.

Die beschränkte Handlungsfähigkeit ist kein Zustand, der sich aussitzen lässt. Wer erst in der Lage klärt, wer entscheidet, hat die Lage bereits verloren.

02

Lernen aus der Praxis

Wo Handlungsfähigkeit abreißt

2.0 – DIE PROBE

Krisen sind der Stresstest für organisationsübergreifende Zusammenarbeit



Acht Lagen sind durchgehend dokumentiert. Fünf wurden gemeistert, drei nicht. Den Ausschlag gab, ob vorher geklärt war, wer entscheidet und handelt. Hybride Angriffe verschärfen das Muster, weil ein Gegner die Zuständigkeitsnahe gezielt ausnutzen kann.

Im Ahrtal kamen Kräfte, Geräte und Hilfsbereitschaft an. Der letzte Kilometer blieb offen: Einheiten standen bereit, während ihre Zuordnung zu Einsatzräumen stockte. Zwischen eingetroffener Fähigkeit und wirksamem Auftrag klappt der Bruch. → [2.1](#)

Am Kachowka-Staudamm lief die Kette unter Kriegsbedingungen durch. Mehr als 10.000 Hilferufe wurden zu rund 700 Einsatzpunkten verdichtet, weil Datenplattform, Prüfung und Führung bereits vor dem Dammbruch verbunden waren. Die Bevölkerung war damit Teil eines vorbereiteten Lagebilds. → [2.2](#)

Neuwied liefert die zweite gebrochene Lage. Der Kreis verfügte über Antennenmast, Satellitentelefone, Analogfunk und geübte Kräfte, vierzig Stunden fehlte dennoch die Übersicht über das Geschehen im Nachbarkreis. Gute Ausstattung trägt nur so weit wie das gemeinsame Lagebild. → [2.3](#)

Hybride Angriffe verschärfen dieses Muster, weil der Gegner Zeitpunkt, Ziel und Schwelle wählen kann. Jede Minute für Attribution und Befugnisklärung wird damit selbst zum Teil der Lage. Die Zuständigkeitsnahe ist keine Verwaltungsfrage, sondern eine Verwundbarkeit. → [2.4](#)

Die Gegenprobe kommt aus fünf gelungenen Lagen: Kachowka sowie vier deutsche Fälle aus Brand, Pandemie, Stromausfall und Energiekrise. Überall war die tragende Regel vor dem Ereignis vorhanden. Auch die Wirtschaft erwies sich als resilient: Lieferketten hielten, Entscheidungen wurden schnell umgesetzt. Entscheidend sind die Bedingungen des Gelingens, nicht der Ereignistyp. → [2.5](#)

Aus allen Fällen bleibt ein Muster zurück: Bewertung und Auftrag sind die empfindlichen Übergänge, der Wiederanlauf ist am schwächsten dokumentiert. Wo Strukturen nicht greifen, tragen Bevölkerung, Ehrenamt und lokale Selbstorganisation die Lage. Ein Beleg für die Improvisationsfähigkeit aus Kapitel 1. → [2.6](#)

2.1 – AHR TAL · JULI 2021

Auf dem letzten Kilometer fehlte die Führung



Hochwasser in Altenahr-Altenburg am 15. Juli 2021

Das Hochwasser verwüstete das Tal. Einheiten aus mehreren Bundesländern trafen innerhalb von zwei Tagen ein. Vor Ort fehlten weder Kräfte noch Hilfsbereitschaft, es fehlte eine Anweisung.

Die Alarmierung funktionierte. Der Reserveoffizier Leonard Wessendorf von Project Q beschreibt das Amtshilfeverfahren als tragfähig. Aktivierung und Alarmierung liefen wie vorgesehen. Die Zusammenziehung seiner Einheiten gelang zuverlässig innerhalb von 24 bis 48 Stunden. Er stellt seiner Schilderung einen Vorbehalt voran: In eine steuernde Meldekette war er selbst nicht eingebunden.

Die Verzögerung entstand nach der Ankunft. In Großlagen wie dieser herrsche zunächst Verwirrung, so Wessendorf. Einweisung und Zuordnung der anrollenden Kräfte erfolgten manuell mit Karten. Das Ergebnis: Fähigkeiten standen an einer Stelle bereit, ohne zu wissen, dass sie andernorts dringend gebraucht wurden. Die Bruchstelle liegt daher hinter der Meldung: in der Zuordnung vor Ort, zwischen Auftrag und Wirkung.

Zwei Umstände verschärften sie. Christian Miller von der Feuerwehr Köln verweist auf die Kommunikationslage: Länderübergreifend stehen ausschließlich die Bundesrufgruppen des behördlichen Digitalfunks zur Verfügung, und die Infrastruktur kann selbst ausfallen. Im Ahrtal waren Basisstationen unmittelbar betroffen. Wer nicht kommunizieren kann, kann auch nicht zuordnen.

Hinzu kam eine ungeplante Ressource. Klaus Ritzgen vom Deutschen Landkreistag beschreibt den Wandel von organisierter Hilfeleistung zu spontaneren Formen, wie er im Ahrtal massiv sichtbar wurde. Spontanhelfende sind wertvoll und schaffen zugleich ein Problem: Sie

erscheinen an der falschen Stelle, erschweren die Gefahrenabwehr und bringen sich selbst in Gefahr.

Nach dem Einsatz wertet jede Organisation für sich aus. Das Land erstellt ein politisches Programm, das Technische Hilfswerk (THW) eine Einsatzanalyse, die Hilfsorganisationen eigene Berichte. Keine übergeordnete Institution betrachtet die Zusammenhänge, die Raumplanung bleibt außen vor. Benni Thiebes vom Deutschen Komitee Katastrophenvorsorge (DKKV) nennt das Ergebnis deshalb nicht „Lessons Learned“. Er spricht von „Lessons to learn“.

Sein Beleg ist der Wiederaufbau. Von rund 8.500 zerstörten oder schwer beschädigten Häusern im Ahrtal, so Thiebes, dürften viele wegen ihrer Lage am Wasser nicht wieder errichtet werden. Versicherungen und Wiederaufbauhilfen gehen dennoch vom Aufbau an gleicher Stelle aus.



„Damit stellen wir genau die Situation wieder her, die vorher zur Katastrophe geführt hat.“

Dr. Benni Thiebes • Geschäftsführer, DKKV

Im Ahrtal fehlte nichts außer der Zuordnung. Kräfte, Geräte und Hilfsbereitschaft waren da, die Meldung kam an — nur nicht der Auftrag. Und was daraus zu lernen war, blieb in getrennten Berichten liegen.

2.2 – KACHOWKA-STAUDAMM · JUNI 2023

Das Lagebild stand, bevor der Damm brach



Der Korabelna-Platz in Cherson nach der Zerstörung des Wasserkraftwerks Kachowka, Juni 2023

Ein Angriff zerstörte den Damm im Juni 2023. Die Flut erreichte Cherson binnen Stunden und traf ein Gebiet unter Kriegsbedingungen. Kräfte und Mittel waren knapp – was funktionierte, war das Lagebild.

Als der Damm brach, existierte in der Ukraine eine Plattform für militärische Datenverarbeitung. Für den Zivilschutz war sie nicht gebaut. Noch am selben Tag arbeitete sie als Rettungswerkzeug. Über Telegram gingen mehr als 10.000 Hilferufe ein, daraus entstanden 700 konkrete Einsatzpunkte für Rettungsteams. Lenkungsausschuss, Referatsabstimmung und Ministeriumspapier waren dafür nicht nötig. Oleksii Teplukhin, einer der Gründer, schilderte den Ablauf 2025 im Interview auf der AFCEA Fachausstellung in Bonn.

Der Umbau gelang, weil die Übergabe bereits gebaut war. Die Plattform folgt vier Schritten: erfassen, strukturieren, analysieren, nutzbar machen. Der letzte entscheidet. Satellitendaten, Drohnenbilder, Funksignale, Beiträge aus sozialen Netzwerken und offene Quellen werden semantisch geordnet und in Kontext gesetzt. Neu war der Adressat, nicht die Erfassung: Anstelle eines Führungsstabs empfingen Rettungsteams das Ergebnis. Diesen Wechsel musste niemand aushandeln.

Eine verbreitete Gegenposition hält eine solche Lösung für zentralistisch und deshalb für unvereinbar mit dem deutschen Föderalismus. Tobias Schönherr von der Bundespolizei widerspricht: Die Verantwortung bleibe in der Ukraine auf lokaler Ebene. Eine Steuerung aus Kiew gebe es nicht, die Oblaste handelten selbstständig. Die Struktur ähnelt der deutschen stärker, als das Bild vom zentral

geführten Kriegsstaat vermuten lässt. Nach Schönherr fehlen hier vorab vereinbarte Verfahren, die eine Entscheidung ermöglichen, ohne im Ereignis sämtliche Zuständigkeiten neu auszuhandeln. Axel Lips von Sopra Steria, der die Absicherung der Olympischen Spiele in Paris begleitet hat, fasst den Befund für Deutschland zusammen.



**„Die Fähigkeiten sind da.
Es geht ums Umsetzen.“**

Axel Lips • Associate Director Public,
Defence & Security, [Sopra Steria](#)

Der Krieg war keine Voraussetzung, er verkürzte den Weg.

Leonard Wessendorff von Project Q kehrt die übliche Dringlichkeitslogik um: Der Übergang zur Landes- und Bündnisverteidigung lasse sich am einfachsten regeln. In der Krise fallen bürokratische Hürden, pragmatische Lösungen setzen sich zügig durch. So seien auch die Ukrainer zu ihrem Vorgehen gekommen. Schwierig sei der Friedensbetrieb: die Frage, wann wer welche Kompetenz einbringen darf.

2.3 – LANDKREIS NEUWIED · JULI 2021

Gut gerüstet, aber ohne Lagebild



Katastrophe Neuwied (Symbolbild)

Der Kreis war besser vorbereitet als die meisten. Eigener Antennenmast, Satellitentelefone, Analogfunk im Kreiseigentum, geübte Verlegeeinsätze. Genützt hat ihm das in der Flutnacht wenig, weil die Vorbereitung an der Kreisgrenze endete.

Neuwied grenzt unmittelbar an den Landkreis Ahrweiler. Am Nachmittag des 14. Juli alarmiert die Leitstelle Koblenz, gegen 17:30 Uhr wird die überörtliche Bereitschaft des Leitstellenbereichs Montabaur aktiviert. Das Ausmaß kennt zu diesem Zeitpunkt niemand. Volker Lemgen von der Kreisverwaltung leitet in dieser Nacht die Funkein-satzzentrale und steuert die Nachalarmierung der Boote. Am Morgen des 15. Juli wechselt er an die Ahr und übernimmt ab 10:00 Uhr einen Einsatzabschnitt.

Zuständig war jeder, ein Lagebild hatte keiner. Lemgens Analyse verwirft die naheliegende Erklärung ausdrücklich. Die Zuständigkeiten waren geregelt: Jeder Leitstellenbereich in Rheinland-Pfalz stellt eine überörtliche Bereitschaft, die Aufsichts- und Dienstleistungs-direktion führt den Einsatz. Das Problem lag anderswo: Niemand wusste, was geschah. Die Behörde übernahm die Einsatzleitung erst am Freitag-mittag, bis dahin organisierten sich die Abschnitte selbst. Lemgen nennt diese Phase eine verlängerte Chaosphase, die bis Samstag andauerte.

Seine Einsatzkräfte erfuhren das tatsächliche Ausmaß erst im Nachgang aus der Presse. Die Ausbildung war nicht das Problem. Ihnen fehlte eine Übersicht, die Ziel und Auftrag erklärte. Auf die Frage, was bei einem vergleichbaren Ereignis zuerst fehlen würde, antwortet Lemgen ohne Zögern: ein schnelles Lagebild.



„Unsere Mannschaft berichtete, dass den Verantwortlichen vor Ort gar nicht bewusst war, was auf sie zukam.“

Volker Lemgen • Sachbearbeiter Brand- und Katastrophenschutz, [Kreis Neuwied](#)

Neuwied setzte die bekannten Lehren aus dem Ahrtal um. Der Kreis baute ein eigenes Brand- und Katastrophenschutz-zentrum auf, das Personal wuchs von drei auf acht Stellen. Das Gebäude verfügt über zwei Heizsysteme und einen Flüssiggastank und bleibt bei Stromausfällen handlungsfähig. Das Land stellt mit dem Brand- und Katastrophenschutzportal ein mehrstufiges Lagebild bereit: Meldungen über Personal, Material und Reserven laufen dort in zwei Zeit-fenstern zusammen, null bis 24 und 24 bis 72 Stunden. Die Kommuni-kation ist gestaffelt abgesichert: behördlicher Digitalfunk, acht Satellitentelefone, ein eigener Antennenmast, Analog- und Gleich-wellenfunk in Eigentum samt Frequenzen, dazu der handschriftliche Vierfachvordruck, der weiterhin geübt wird.

Neuwied schuf diese Vorsorge innerhalb bestehender Zuständig-keiten und ohne neue Behörde. Ausschlaggebend war die Ent-scheidung, nicht ein Strukturwechsel. Sie fiel auf kommunaler, nicht staatlicher Ebene.

2.4 – HYBRIDE LAGEN · UNTERHALB DER SCHWELLE

Wer angreift, muss keine Zuständigkeit klären



Symbolbild © KI generiert (Friedrich)

Naturkatastrophen kennen keine Absicht. Ein Gegner schon. Er wählt den Zeitpunkt, das Ziel und die Schwelle – und er wählt sie so, dass die Klärung der Zuständigkeit länger dauert als sein Angriff.

Ein Anbieter von Leittechnik wurde vor Kurzem über Tage bis Wochen von einem Cyberangriff lahmgelegt. Der Energieversorger EnBW, der diese Technik einsetzt, war nicht das Ziel. Getroffen wurde er trotzdem: Bernd Calaminus von EnBW schildert, dass man die Verbindung zum Anbieter sofort trennte, um sich nicht zu infizieren. Damit blieben die täglichen Aktualisierungen aus, und der eigene Betrieb wurde schwieriger. Die Schutzmaßnahme war zugleich der Schaden.

Der gezielte Angriff kennt kein Ende der Lage. Bernd Reitmeier von Bechtle stellt beide Ereignistypen nebeneinander: Die Flut war ein Ereignis von ein bis zwei Tagen, danach begann der Wiederaufbau. Eine hybride Bedrohung ist zeitlich nicht strukturiert. Sie zielt auf das schwächste Glied, und während die Infrastruktur wiederhergestellt wird, treten weitere Störungen ein. Vorbereiten lasse sich darauf nur, indem man den Stressfall übt.

Die Unklarheit beginnt vor der Entscheidung. Hans-Martin Zimmermann von Airbus Defence and Space beschreibt es aus Sicht dessen, der reagieren müsste: Der Operateur vor dem Bildschirm weiß oft nicht, ob er zuständig ist. Gilt der Vorgang der eigenen Liegenschaft oder dem benachbarten Umspannwerk? Ein Jugendstreich oder ein Angriff, eine akute Bedrohung oder langfristige Aufklärung? Ein Einzelner oder ein ausländischer Staat? An jede Antwort knüpfen sich andere Zuständigkeiten. Der Gegner muss keine davon klären.

Wer meldet, bekommt keine Rückmeldung. Frank Scholz von MilDef beschreibt den Bruch aus der Sicht eines mittelständischen Herstellers. Seine Unternehmensgruppe war bereits angegriffen worden, mit

Ausfällen, deren Urheber sich nicht zuordnen ließen. Staatliche Unterstützung oder Beratung blieb aus. Als Lieferant unterschreibe man die Erfüllung des Grundschutzes als Qualifikationsvoraussetzung, ohne dafür Förderung oder Kostenübernahme zu erhalten.



„Man hat die Pflicht, das festzustellen und zu melden – und was passiert dann? Dann gibt es nichts.“

Frank Scholz • Geschäftsführer, MilDef

Die Schwelle liegt niedrig. Armin Schaus vom Operativen Führungskommando der Bundeswehr benennt vier Linien: Desinformation, strategische Cyberangriffe, Ausspähung und Sabotage. Niemand sei ausgenommen, nur weil er thematisch fernliege. Michael Kreinest von BG Kliniken Ludwigshafen beschreibt die niedrige Schwelle: Zwei durchtrennte Kabel legen eine Schnellfahrstrecke über Tage still, ein Brandanschlag einen ganzen Stadtteil. Diese Angriffe würden sich eher intensivieren, unabhängig davon, ob ein Bündnis- oder Verteidigungsfall vorliegt.

2.5 – DIE GEGENPROBE

Vier Lagen, erfolgreich gemeistert



In Meppen führte ein Stab, in Berlin schuf eine Rechtsverordnung das Mandat, in Ludwigshafen war der analoge Behelf vorgedacht, in der Energiekrise standen die Eskalationsstufen. Keine dieser Regelungen entstand in der Lage.

Moorbrand Meppen 2018

Feuer auf einem Truppenübungsplatz, mehrere Wochen Einsatz

Auf einem Truppenübungsplatz breitete sich 2018 ein Feuer großflächig aus. Christian Miller von der Feuerwehr Köln war im Stab und als Stabsleiter eingesetzt. Er koordinierte das Zusammenwirken der Kräfte im Raum: Bundeswehr, kommunale Kräfte, überörtlicher Katastrophenschutz, Technisches Hilfswerk sowie Landes- und Bundesbehörden. Bis zu 2.500 Einsatzkräfte waren in Operations- und rückwärtigen Bereitstellungsräumen gebunden.

Ein Stab führte, was auf dem Papier verschiedene Welten sind. Die zivil-militärische Zusammenarbeit gelang, weil sie einer gemeinsamen Führung unterstand statt einer Abstimmung zwischen Führungen. Miller ist der einzige Gesprächspartner im Material, der diese Konstellation aus eigener Leitungsverantwortung schildert.



„Katastrophenschutz ist Ländersache, deshalb gibt es im föderalen System derzeit keine Strukturen den Katastrophenschutz länderübergreifend zu führen.“

Christian Miller • Leiter, Feuerwehr Köln

Übertragbar ist daran die Konstruktion, nicht das Ereignis. Miller benennt zugleich, warum sie die Ausnahme blieb: Aus der grundgesetzlichen Zuständigkeit der Länder folgen sechzehn Systeme des Katastrophenschutzes, je nach Land unterschiedlich aufgestellt. Bayern verlangt den förmlichen Rechtskreiswechsel durch Erklärung

des Katastrophenfalls, Nordrhein-Westfalen hat kein eigenes Katastrophenschutzgesetz und benötigt keine förmliche Feststellung. Unterschiedliche Rechtsgrundlagen und Definitionen erschweren schon den Vergleich einsatztaktischer Werte über Landesgrenzen hinweg. In Meppen wurde die gemeinsame Führung hergestellt, weil ein Truppenübungsplatz die Zuständigkeiten ohnehin kreuzte. Ohne diesen Anlass entsteht sie nicht von selbst.

Zentrale Patientenverteilung Berlin ab 2020

Charité koordiniert Intensivbetten in der Pandemie

Der Senat beauftragte die Charité per Rechtsverordnung, die Verteilung schwerkranker Covid-Patienten zu koordinieren. Die Krankenhäuser wurden in einem transparenten Verfahren nach drei Fähigkeitsstufen eingeteilt. Zu den Spitzenzeiten waren alle Intensivbetten belegt. Zu Triage-Entscheidungen kam es nicht, weil jeder Patient dem passenden Versorgungsniveau zugewiesen wurde.

Ein Rechtsakt schuf das Mandat, ein Verfahren die Transparenz.

Leif Erik Sander von der Charité, der das Konzept begleitete, hält es für die wahrscheinlich beste Lösung dieser Art in Deutschland. Es hat sich über mehrere Jahre bewährt.

Beide Elemente waren nötig. Die Rechtsverordnung allein hätte eine Zuständigkeit geschaffen, aber keine Grundlage für die Verteilung. Die Fähigkeitsstufen allein hätten Transparenz erzeugt, aber niemanden ermächtigt, danach zuzuweisen. Erst zusammen entstand ein Verfahren, das unter Volllast trug. Das ist die am ehesten übertragbare der vier Bedingungen: Sie kommt ohne neue Institution aus, ohne zusätzliches Personal und ohne Technik, die es nicht schon gab.



„Es ging nur, weil es zentral wirklich koordiniert wurde und transparent war, wer was kann.“

Leif Erik Sander • Klinikdirektor, Mitglied im Expertenrat Gesundheit und Resilienz, [Charité](#)

Stromausfall Ludwigshafen 2023

Großstadt sechs Stunden ohne Strom, Wiederanlauf über Tage

Ein Großteil der Stadt verlor die Elektrizitätsversorgung. Am eindrücklichsten war für Michael Kreinest von der BG Klinik der Zusammenbruch der Telekommunikation: Die Mobilfunkmasten standen still. Das Mobiltelefon lief über den Akku, telefonieren ließ sich nicht, das Internet war weg, der Funk nur eingeschränkt nutzbar. Krankenhäuser sind in der Regel nicht an das Funknetz des Rettungsdienstes angebunden.

Ein Alarm- und Einsatzplan lag vor. Niemand musste bei null anfangen. Der analoge Behelf funktionierte: Boten und eine Motorradstaffel fuhren die Kliniken sowie die übrige kritische Infrastruktur des Gesundheitswesens ab. Vor den Krankenhäusern wurden Rettungswagen platziert, deren Funk als Verbindung zur Leitstelle diente. Der Rückfall auf eine niedrigere Technikstufe war vorgedacht, nicht improvisiert.

Die Bedingung endete dort, wo der Strom zurückkam. Kreinest lernte in dieser Lage etwas, das er zuvor nicht bedacht hatte: Nach der Rückkehr des Stroms läuft nicht einfach alles wieder. Server müssen in einer bestimmten Reihenfolge hochfahren, vieles von Hand gestartet werden. Brandschutztüren fallen bei Stromausfall zu und müssen einzeln freigegeben werden – in einem großen Krankenhaus eine Arbeit von Tagen.

Auch Wohngebäude bleiben nach der Rückkehr des Stroms gestört. In Hochhäusern fällt oberhalb des dritten Stocks das Wasser aus, weil die Pumpen stehen. Heizungen müssen vielfach händisch zurückgesetzt werden. In einem strengen Winter musste ein Techniker dafür durch jedes Mehrfamilienhaus, was Monate dauert. Es ist der einzige detaillierte Befund zum Wiederanlauf im gesamten Material – für einen Übergang, den sonst niemand verantwortet.

Energiekrise 2022

Gaslieferungen bleiben aus, ein Sommer Krisensteuerung

Russland drehte den Gashahn zu. Die Bundesregierung war nicht vorbereitet, und der Ausfall bedeutete mehr als kalte Wohnungen: Viele Industrieanlagen lassen sich nicht einfach herunterfahren, ein Stopp hätte sie dauerhaft beschädigt. In dieser Lage rief der Bundeskanzler eine kleine Gruppe von Spitzenbeamten und Regierungsmitgliedern zusammen. Treffpunkt war ein abhörsicherer Raum im Kanzleramt, mit stählerner Tür und manueller Verriegelung. Daher der spätere Spitzname.

Ein kleiner Kreis entschied, statt abzustimmen. Die Gruppe organisierte binnen weniger Tage den globalen Ankauf von Flüssiggas. Sie gründete eine Tarnfirma, schloss Verträge rund um den Globus und ließ Terminals in Monaten bauen – für Infrastrukturprojekte dieser Art vergehen in Deutschland sonst Jahre. Der Speicherstand lag bis zum Winter über 90 Prozent, die Notfallstufe wurde nie ausgerufen, die Industrie kam ohne Produktionsausfälle durch.

Darunter arbeitete eine Ebene, die im Vorgriff plante. Paul Höller aus dem nordrhein-westfälischen Wirtschaftsministerium beschreibt sie: Anders als zu Beginn der Pandemie, als zuerst geschlossen und im laufenden Herunterfahren nachgedacht wurde, waren diesmal Bezugsberechtigung und Rationierung vorher durchdacht. Über Füllstände und Lieferbedingungen wurde täglich berichtet, in ebenen- und ressortübergreifenden Arbeitskreisen zwischen Bundesregierung, Bundesnetzagentur und Ländern.

Auf der Betreiberebene setzte sich die schnelle Umsetzung fort.

Bernd Calaminus von der EnBW schildert das Kohlelager Germersheim: Auf Geheiß des Übertragungsnetzbetreibers durfte das Unternehmen dort rund 100.000 Tonnen Kohle einlagern – in Rheinland-Pfalz, einem Land, das selbst keine Kohleanlage betreibt –, um sie im Süden verfügbar zu halten. Politischer Wille verkürzte Verfahren, die sonst sehr viel länger dauern.

Die Gegenprobe reicht in die Wirtschaft. Der Handel stabilisierte nach den ersten Lieferkettenbrüchen der Pandemie die Versorgung und passte Beschaffung, Alternativen und Energieverbrauch dauerhaft an. Kai Hudetz vom IFH Köln fasst die Voraussetzung so: „Verfügbarkeit ist nicht gottgegeben – sie ist das Ergebnis funktionierender Lieferketten.“ Axel Lips zieht aus der Absicherung der Olympischen Spiele 2024 in Paris dieselbe Umsetzungslinie für Sicherheitsfähigkeiten: „Die Fähigkeiten sind da. Es geht ums Umsetzen.“

2.6 – DAS MUSTER

Erkannt, dokumentiert, folgenlos

Besonders oft versagen die Bewertung eines Signals zum Lagebild und die Übersetzung einer Entscheidung in einen Auftrag.

An diesen Stellen scheiterten die dokumentierten Bruchfälle. Im Ahrtal kam die Zuordnung vor Ort hinzu, bei hybriden Lagen die Befugnisklärung.

Durchweg unvorbereitet bleibt der Wiederanlauf. Er taucht nur in Ludwigshafen auf – als Überraschung. Michael Kreinest von den BG Kliniken Ludwigshafen lernte dort, dass nach der Rückkehr des Stroms nichts von selbst wieder anläuft. In den übrigen sechs Lagen erscheint diese Phase weder als Erfolg noch als Bruch.

Jeder Positivfall beruhte auf einer vorher geschaffenen Bedingung. Ein kommunaler Stab, ein Senat per Verordnung, ein Krankenhaus mit eigenem Einsatzplan, ein Kanzleramtskreis unter maximalem Druck. Dafür brauchte es weder neue Technik noch eine Gesetzesänderung – und drei dieser vier Stellen hatten keinen Auftrag für gesamtstaatliche Vorsorge.

Eine zweite Linie verbindet die gelungenen Lagen. Bevölkerung und freiwillige Kräfte liefern Information, Personal und lokale Handlungsfähigkeit. In Kachowka wurden Hinweise aus der Bevölkerung zu konkreten Einsatzpunkten. In den deutschen Lagen tragen Ehrenamt und Selbstorganisation die Bewältigung. Kapitel 7 übersetzt diese Mitwirkung in konkrete Maßnahmen im Handlungsfeld Gesellschaft, Kultur und Üben. → 7.7

Das Muster ist bekannt, und es bleibt folgenlos. Ein Planspiel zum großflächigen Stromausfall, das Armin Fleischmann gemeinsam mit dem Auswärtigen Amt für alle Ressorts durchführte, ergab: Nur drei Ressorts hatten überhaupt Vorsorge getroffen. Das Ergebnis beruht auf einer Übung, nicht auf einer Vermutung.



„Lessons Learned habe ich aus meinem Vokabular gestrichen. Es gibt bei mir nur noch Lessons Identified.“

Armin Fleischmann • Generalmajor und Vorsitzender, AFCEA Bonn e.V.

Geübte Szenarien traten im Schnitt zwei bis vier Jahre später real ein. Diese Faustregel gilt laut Martin Zeidler vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) seit 2006. Es fehlt nicht am politischen Willen und nicht an der Analyse – die Auswertungsberichte werden veröffentlicht und an Länder und Akteure weitergegeben. Was fehlt, ist die Übersetzung in eigenes Handeln und ein Monitoring der Umsetzung.

Damit steht die Aufgabe für die folgenden Kapitel fest. Die Brüche sind bekannt, die Gegenmittel erprobt, die Erkenntnisse dokumentiert. Was fehlt, ist die Stelle, die sie verbindlich macht.

FALLANALYSE

Acht Lagen, fünf Übergänge: Es bricht immer dazwischen

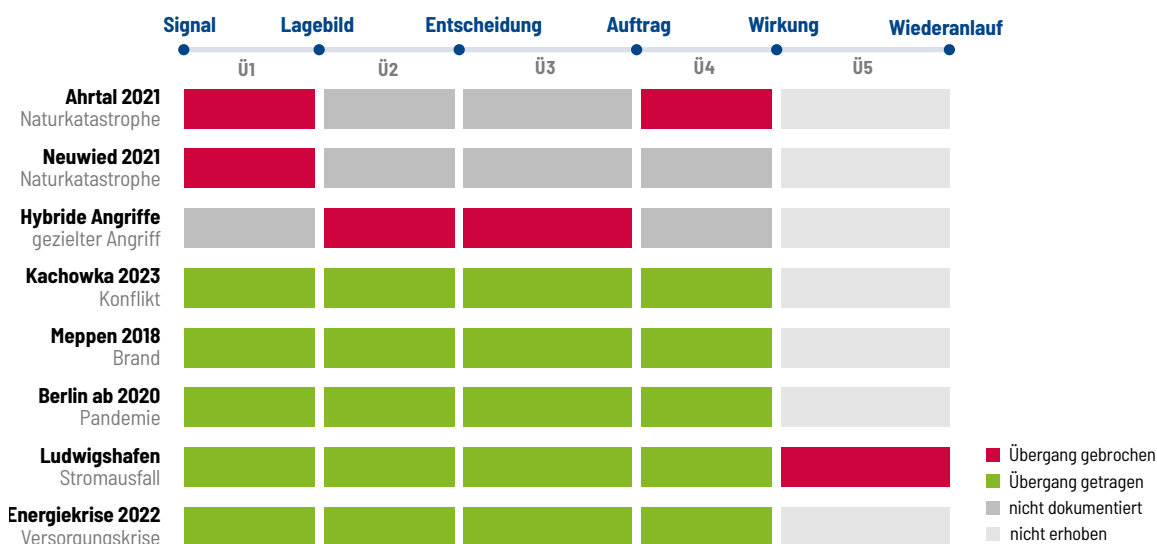


Abb. 2.1: Interview-Auswertung und Beispieldatenbank GSÖ 2030

03

Das Zielbild

**Ein Sicherheits-
ökosystem, das
Wirkung erzielt**

3.0 – DER RICHTUNGSWECHSEL

Was fehlt, ist der Auftrag – nicht eine neue Behörde



Wer eine Sicherheitsarchitektur entwirft, braucht zuerst eine Zielmarke: Welche Wirkung soll gemeinsam entstehen? Kapitel 3 übersetzt die Befunde in vier Wirkungsversprechen, einen klaren Geltungsbereich, eine Wirkungsarchitektur und sieben Fähigkeiten. Danach kommt die Probe: ein internationaler Vergleich und sechs prüfende Fragen.

Vier Wirkungsversprechen geben die Richtung vor: frühere Lageerkennung, schnellere und bessere Entscheidungen, wirksames Handeln und höhere Durchhaltefähigkeit. Sie beschreiben den gemeinsamen Nutzen, an dem jede spätere Rolle und Technik gemessen wird. Die Zielmarke steht damit, bevor Zuständigkeiten verteilt werden. → [3.1](#)

Der Verbund soll im Alltag keine zusätzliche Ebene erzeugen. Er greift an Kippunkten: bei ressortübergreifender Wirkung, Kaskaden, zu kurzen Entscheidungsfenstern und Lagen, die verbindliche Koordination verlangen. Der Geltungsbereich bestimmt sich über die Dynamik der Lage. → [3.2](#)

Krisen verlaufen in überlagernden Zeiträumen. Vorbereitung, operative Bewältigung sowie Wiederanlauf und Lernen müssen gleichzeitig gedacht werden, damit eine Entscheidung in der einen Phase die nächste nicht blockiert. Diese Bewegung ordnet die Wirkungsarchitektur. Die Orchestrierung verläuft durchgängig durch sie hindurch. → [3.3](#)

Aus dieser Architektur folgen sieben Fähigkeiten: erkennen, bewerten, entscheiden, koordinieren, handeln, durchhalten sowie wiederherstellen und lernen. Bevölkerung und freiwillige Kräfte erweitern diese Fähigkeiten dort, wo sie als Sensor, Helfer und lokale Reserve vorbereitet sind. Das Können des Systems steht damit fest, bevor Akteure zugeordnet werden. → [3.4](#)

Der internationale Vergleich setzt einen äußeren Maßstab. Deutschland erreicht 14 von 30 Punkten, sechs der zehn Dimensionen liegen im frühen Aufbaustand, und die größten Abstände betreffen Steuerung und Durchhaltefähigkeit. Die Zeitabstände zu den Referenzländern sind redaktionelle Ableitungen und als solche gekennzeichnet. → [3.5](#)

Ein Zielbild wird erst durch überprüfbare Ansprüche brauchbar. Sechs Fragen prüfen Zielniveau, Vorsorge, Priorisierung, Wiederanlauf, Durchhaltezeit und den Preis der Resilienz. Am Ende steht die Frage, die über alle weiteren Kapitel entscheidet: Wie gut wollen wir sein? → [3.6](#)

ZIELBILD

Gesamtstaatliches Sicherheitsökosystem 2030

Sieben Ebenen: wofür das System da ist, wie es arbeitet und womit.

KERN

EBENE 1 Wirkungsversprechen

Voraussetzung für Wirkung – kein Zusatznutzen

W1 Frühere Lageerkennung

W2 Schnellere & bessere Entscheidungen

W3 Wirksames Handeln

W4 Höhere Durchhaltefähigkeit

EBENE 2 Geltungsbereich und Kippunkte

Wirkungstrieb, nicht bedrohungstypengetrieben

G1 Ressortübergreifend

G2 Kaskadierende Effekte

G3 Zeitkritische Entscheidungen

G4 Orchestrierung erforderlich

EBENE 3 Wirkungsarchitektur

Keine linearen Schritte – sondern parallele Dimensionen

DAVOR Antizipation & Vorbereitung

DABEI Bewältigung & operative Wirkung

DANACH Wiederanlauf & Lernen

EBENE 4 Fähigkeiten

Was das System können muss – nicht, wer es tut

F1 Lage erkennen & antizipieren

F2 Lage bewerten & priorisieren

F3 Entscheiden & ausrichten

F4 Koordinieren & führen

F5 Wirksam handeln

F6 Durchhaltefähigkeit sichern

F7 Wiederherstellen & lernen

EBENE 5 Rollen und Verantwortung

Kein Akteur ist exklusiv – kein Steuerungsapparat

R1 Strategische Führung

R2 Operative Koordination

R3 Behörden und Einsatzkräfte

R4 Infrastrukturbetreiber

R5 Lagebild und Datenaustausch

R6 Durchhaltefähigkeit & Wiederanlauf

EBENE 6 Digitales Rückgrat

Kein IT-Projekt – technologische Voraussetzung staatlicher Wirkung

D1 Lagebild & Sensorik

D2 Datenintegration & Interoperabilität

D3 Kommunikation & Vernetzung

D4 Führungs- & Entscheidungsunterstützung

D5 Cyber- & Informationssicherheit

D6 Logistik- & Ressourcensteuerung

D7 Resilienz & Wiederanlauf

D8 Governance & Zugriff

EBENE 7 Innovationsraum

Technologischer Vorsprung als Antwort auf veränderte Krisen

I1 Vernetzte Krisenführung

I2 Cyber- & Informationssicherheit

I3 KI & Entscheidungsunterstützung

I4 Autonome & unbemannte Systeme

I5 Weltraum & Satellitensysteme

I6 Energie, Versorgung & Logistik

I7 Sensorik & Aufklärung

I8 Dual-Use-Ökosysteme

SYSTEME

WERKZEUGE

Sieben Ebenen - Zielbild Gesamtstaatliches Sicherheitsökosystem 2030

Abb. 3.1: Zielbild GSÖ 2030

Das Zielbild: vom Nebeneinander der Akteure zur gemeinsamen Wirkung

Auf ein Koordinationsproblem folgt gewöhnlich der Ruf nach einer neuen Institution. In Deutschland würde eine Zentralbehörde für gesamtstaatliche Sicherheit jedoch Zuständigkeiten zwischen Bund und Ländern verschieben und damit die Verfassung berühren. Das Sicherheitsökosystem 2030 folgt einem anderen Prinzip: Ein nachvollziehbarer gemeinsamer Nutzen hält die Beteiligten zusammen, ohne eine zusätzliche Hierarchiestufe einzuziehen. Er bindet dauerhaft, gibt Orientierung und verhindert unter Druck den Rückfall in isolierte Einzelinteressen. Diese Funktion übernimmt andernorts die Weisung.

Finnland zeigt, dass dieses Prinzip trägt – als Governance-Modell, nicht als Behörde. Seit 2003 schützt das Modell der umfassenden Sicherheit die lebenswichtigen Funktionen der Gesellschaft im Zusammenwirken von Behörden, Wirtschaft, Organisationen und Bevölkerung. Die jüngste Fassung wurde im Januar 2025 als Regierungsbeschluss verabschiedet. Ein jährlicher Bericht an die Regierung macht Fortschritt und Lücken sichtbar. Ohne Rechenschaft bliebe der Auftrag folgenlos.

Das Modell entstand in drei Schritten. Den Ausgangspunkt bildeten internationale Referenzrahmen: die sieben Baseline Requirements der NATO zur zivilen Resilienz, das finnische Modell, das National Preparedness Goal der Vereinigten Staaten und die niederländische Ordnung der Sicherheitsregionen. Werkstätten mit den Studienpartnern übertrugen diese Ansätze auf die föderalen Bedingungen Deutschlands. Die Feldphase prüfte jedes Element an 55 Tiefeninterviews und einer Befragung unter 72 Technologieanbietern und Anwendern. Nicht bestätigte Elemente wurden gestrichen.

Entscheidend ist die Reihenfolge. Der deutsche Sicherheitsdiskurs beginnt meist bei der Zuständigkeit und leitet daraus das Handeln ab. Das Modell dreht die Logik um: Zuerst wird das geschuldete Ergebnis bestimmt, danach der verantwortliche Träger. Zuständigkeit bleibt erhalten, folgt aber aus der Aufgabe.

Das Zielbild führt diese Reihenfolge in sieben Ebenen aus. Sie beantworten drei Fragen: wofür das System da ist, wie es arbeitet und womit.

- » **Der KERN.** Ebene 1 benennt die vier Wirkungsversprechen, Ebene 2 den Geltungsbereich und die Kippunkte, an denen der Verbund greift.
- » **Die SYSTEME.** Ebene 3 ordnet die Wirkungsarchitektur in DAVOR, DABEL und DANACH, Ebene 4 die sieben Fähigkeiten, Ebene 5 Governance, Rollen und Verantwortung.
- » **Die WERKZEUGE.** Ebene 6 beschreibt das digitale Rückgrat mit acht Technologie-Domänen, Ebene 7 den Innovationsraum.

Die ersten vier Ebenen sind Gegenstand des vorliegenden Kapitels. Die letzten drei tragen so viel Gewicht, dass sie eigene Kapitel verlangen. Kapitel 4 klärt, wer im Verbund welches Mandat trägt. Kapitel 5 beschreibt das digitale Rückgrat, über das die Beteiligten verbunden sind. Kapitel 7 öffnet den Innovationsraum für Technologien, die noch nicht in der Fläche verfügbar sind.

3.1 – DAS WIRKUNGSVERSprechen

Vier Leistungen, die keiner allein erbringt

Zeitgewinn, klare Prioritäten, abgestimmte Umsetzung und gesicherte kritische Funktionen bilden das gemeinsame Versprechen. Bestehende Fähigkeiten, Rollen und Ressourcen werden dafür verbindlich zusammengeführt.

Rechtzeitige Lageerkennung verschafft Vorsprung, weil kein Akteur allein über alle Signale verfügt. Österreichs nationale Abwasserüberwachung erfasst 94 Gemeinden mit mehr als 59 Prozent der Bevölkerung. Den Wechsel der vorherrschenden Virusvariante zeigte sie vor der klinischen Sequenzierung an.

Entscheidungen gewinnen an Tempo und Qualität, sobald Prioritäten vorab geklärt sind. Im deutschen Energiesystem fehlt diese Ordnung: Die Abschaltpläne nennen keine Rangfolge einzelner Unternehmen, obwohl kritische Lebensmittelbetriebe genau damit rechnen.

Gemeinsames Handeln nutzt vorhandene Kapazitäten besser. Im niederländischen Landelijk Crisis Management System arbeiten Feuerwehr, Polizei, Gesundheitsdienste und Gemeinden auf einer

Plattform. Die nationale Koordinierungsstelle lenkt überregionale Einsätze auf dieser Grundlage.

Größere Durchhaltefähigkeit lässt sich schrittweise aufbauen. Estland sichert seine Verwaltung als digitale Botschaft in ausländischen Rechenzentren. Bei Besetzung oder Cyberangriff kann die Regierung von dort weiterarbeiten.

Sinnvoll orchestrieren führt alle vier Verbesserungen zusammen. Als Querschnitt überschreitet es Organisationsgrenzen und macht aus einzelnen Beiträgen eine gemeinsame Leistung.

Vom Nebeneinander der Akteure zur gemeinsamen Wirkung – nicht durch neue Strukturen, sondern durch verbindliche Übergaben.

EBENE 1

Vier Versprechen, an denen sich alles messen lässt

Voraussetzung für Wirkung – kein Zusatznutzen

W1

Frühere Lageerkennung

Verdichtete Lageinformationen über Akteurs- und Ressortgrenzen hinweg – Frühwarnung, bevor Eskalation einsetzt.

W2

Schnellere & bessere Entscheidungen

Abgestimmte Priorisierung schlägt die formale Abstimmungsschleife. Entscheidungsvorsprung statt Rückstand.

W3

Wirksames Handeln

Weniger Reibung zwischen Akteuren. Bestehende Fähigkeiten werden systemisch zugänglich statt einzeln optimiert.

W4

Höhere Durchhaltefähigkeit

Lose Kopplung begrenzt Kaskaden. Die Vielfalt der Akteure ist Resilienzfaktor, nicht Nachteil.

Abb. 3.2: Zielbild GSÖ 2030, Ebene 1

3.2 – DER GELTUNGSBEREICH

Die Dynamik entscheidet über den Geltungsbereich

Der Verbund greift erst, sobald bestehende Routinen ihre Wirksamkeit verlieren. Dieser Auslöser muss vor dem Ereignis feststehen. Eine Regelung für jede Alltagslage würde das Modell überdehnen.

Vier Bedingungen kennzeichnen den Übergang. Im Bremer Drohnenfall liefen fünf Ressorts parallel, während keines allein eine Bewertung vornehmen konnte. Am 8. Oktober 2022 legten zwei durchtrennte Glasfaserleitungen in Herne und Berlin das Zugfunksystem GSM-R lahm, binnen Minuten stand der Verkehr in vier Bundesländern für rund drei Stunden. Im Ahrtal ließen etwa 200 Liter Regen pro Quadratmeter das Entscheidungsfenster auf wenige Stunden schrumpfen. Beim Bruch des Kachowka-Staudamms lag der Zivilschutz formal beim Staatlichen Notdienst, die tatsächliche Koordination übernahm das Digitalministerium. Sind sie überschritten, greifen bestehende Routinen nicht mehr – die Grafik zeigt, woran das erkennbar ist.

In der Praxis entscheidet die Schwelle über Stunden. Bundesweit ist nicht einheitlich geregelt, wann die Verantwortung vom Landrat auf das Innenministerium übergeht. Als ungeschriebene Faustregel gelten drei betroffene Landkreise. Nach Norbert Ahrends Beschreibung kann bis zur koordinierten Entscheidung ein Tag vergehen. Ähnlich verläuft die Erstmessung chemischer, biologischer, radiologischer und nuklearer Gefahren: Der Unterstützungsverbund des Bundes wäre binnen einer Stunde einsatzbereit, doch die Anforderung muss von

der Rettungsleitstelle über Landrat und Innenministerium laufen und anschließend den gesamten Weg zurücklaufen.



„Wenn die Schwellen – wer wann wie eingreifen darf – erst im Ernstfall ausgehandelt werden, dann ist es zu spät.“

Benedikt Meng • Leiter Business Development & Strategie, [infodas](#)

Genauso wichtig ist die Grenze. Alltägliche Routinen und Lagen ohne übergreifende Dynamik verbleiben in der bestehenden Zuständigkeit. Ein Modell für jeden Fall wäre in keinem Fall verbindlich. Die Erhebung zeigt zugleich, welche Konstellation die Praxis vor Augen hat: Jeder zweite Befragte wählt die hybride Bedrohung als Anker.

Damit richtet sich der Geltungsbereich nach der Dynamik einer Lage. Der Bedrohungstyp allein entscheidet ihn nicht. Welche Leistung dann gefordert ist, zeigt Abschnitt 3.4.

EBENE 2

Kippunkte bestimmen, wann der Verbund greift

Wirkungsgetrieben, nicht bedrohungstypengetrieben

G1

Ressortübergreifend

Wirkungen überschreiten Ressort-, Ebenen- und Sektorgrenzen. Kein Akteur hat den vollständigen Überblick.

G2

Kaskadierende Effekte

Der Ausfall einer Funktion zieht weitere nach sich. Wechselwirkungen bestimmen das Lagebild.

G3

Zeitkritische Entscheidungen

Das Entscheidungsfenster ist kleiner als der Abstimmungsaufwand. Bestehende Routinen greifen nicht.

G4

Orchestrierung erforderlich

Zivile, staatliche und militärische Beiträge müssen zusammenwirken – ohne klare Führungslogik.

AUSSERHALB DES GELTUNGSBEREICHS

Routine- und Alltagslagen mit klarer Zuständigkeit · militärische Einsatz- und Gefechtsführung · Lagen, in denen bestehende Routinen noch wirken

Abb. 3.3: Zielbild GSÖ 2030, Ebene 2

3.3 – DIE ARCHITEKTUR

Erst die Wirkung, dann die Struktur

Eine lange Krise verläuft nie in sauber getrennten Abschnitten. Vorbereitung, akuter Einsatz und Rückkehr in den Normalbetrieb überlagern sich. Das Zielbild nennt sie Davor, Dabei und Danach – keine Schritte, sondern gleichzeitig zu bearbeitende Dimensionen.

Das hat praktische Folgen. Abgeschlossene Vorbereitung steht im Ereignis nicht automatisch zur Verfügung. Erkenntnisse, die erst nach dem Einsatz ausgewertet werden, erreichen die nächste Lage zu spät.

Davor entscheidet die Vorbereitung über das Tempo im Ereignis.

Japans J-ALERT erreicht binnen vier Sekunden Fernsehen, Radio, Sirenen, Lautsprecherwagen und Mobiltelefone – Erdbeben, Tsunami, Taifun und Raketenwarnung über denselben Weg. Diese vier Sekunden sind keine technische, sondern eine organisatorische Leistung: Zuständigkeiten, Formate und Kanäle waren vorher geklärt.

Dabei entsteht Wirkung aus der Verbindung, nicht aus dem einzelnen Mittel.

In Kalifornien überwachten Drohnen mit Wärmebildkameras nachts die Brandherde und übertrugen Live-Bilder über eine Geoplattform in die Zentralen. Daraufhin setzte ein Einsatzleiter 400 Feuerwehrleute gezielt um. Drohne, Plattform und Zentrale gehörten verschiedenen Stellen.

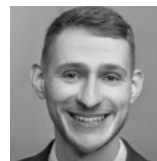
Danach ist die Rückkehr in den Normalbetrieb am schwächsten vorbereitet.

Nach dem NotPetya-Angriff 2017 fand Maersk in Ghana eine Sicherungskopie, die zufällig vom Netz getrennt war: 45.000 Rechner, zehn Tage bis zur Wiederherstellung, rund 300 Millionen Dollar Schaden. Getragen hat kein Verfahren, sondern ein Zufall.

Durchgängige Orchestrierung hält die drei Phasen zusammen. Sie ist keine eigene Phase, sondern die Voraussetzung dafür, dass die drei ineinandergreifen. Vier Faktoren tragen über den gesamten Verlauf:

- » verbindliche Steuerung und Entscheidungsfähigkeit, wie sie der Gasnotfallplan 2022 mit seinen vorab definierten Eskalationsstufen zeigte.
- » eine befähigte Bevölkerung, die nicht erst im Ernstfall lernt, was von ihr erwartet wird.
- » ein gemeinsames digitales Rückgrat, wie es Brandenburg nach den Waldbränden 2018 mit einer BOS-weiten Informationsplattform aufgebaut hat.
- » rollenklare Zusammenarbeit über Zuständigkeitsgrenzen hinweg – etwa im Kooperationsvertrag, der die Verwundetenrücktransporte zwischen Hilfsorganisationen und Sanitätskommando regelt.

Fehlt einer davon, lassen sich die zuvor vorgestellten Wirkungsversprechen nicht einlösen, weil dann niemand die Übergänge verantwortet.



„Da gibt es kein Rotes Kreuz, keine Ehrenamtlichen – da kommt nicht der Landwirt mit dem Traktor und packt mit an.“

Dr. Christian Stuffrein • Referatsleiter, Deutscher Landkreistag

EBENE 3

Wirkungsarchitektur

Keine linearen Schritte – sondern parallele Dimensionen

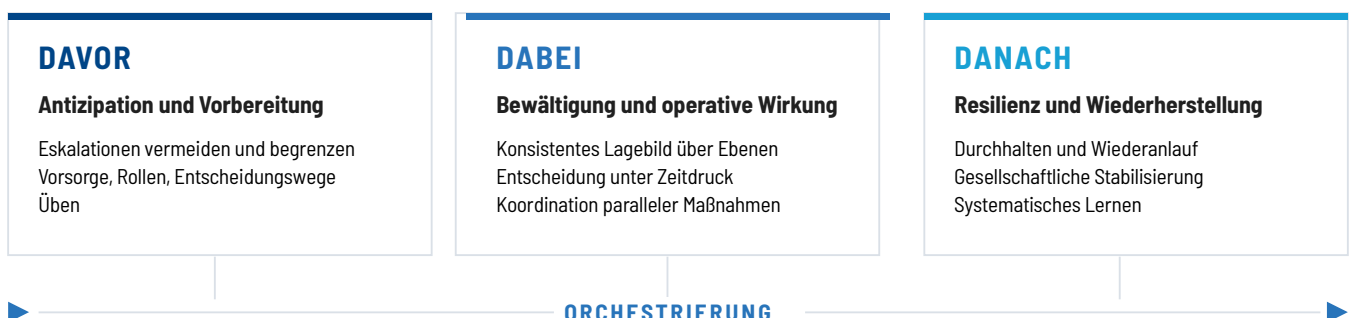


Abb. 3.4: Zielbild GSÖ 2030, Ebene 3

So wird die Verkettungslücke geschlossen

Zwischen den Phasen fehlt heute die Verbindung. Werkzeuge erfassen Signale oder entfalten Wirkung, die Vermittlung dazwischen bleibt nahezu unbesetzt. Ein Inventar führt keine Krise. Entschieden wird dort, wo ein Lagebild in Führung übersetzt wird.

Die Befragung macht die Verkettungslücke sichtbar: Von 48 Wirkungsnennungen entfallen 17 auf das Erkennen und 22 auf das Handeln – zusammen 81 Prozent an den beiden Enden der Fähigkeitskette. Für Bewerten, Entscheiden und Koordinieren bleiben fünf. Das Orchestrieren, das die ganze Kette zusammenhalten müsste, kommt auf eine einzige Nennung.

Die Interviews verorten den Bruch genauer. 13 Gesprächspartner nennen die Strecke zwischen Kommune, Land und Bund als wichtigste Bruchstelle. Zuerst versagt die Verbindung der Systeme, fehlende Kapazität folgt dahinter. Beim Zeitverlust verweisen 18 auf Föderalismus und Ebenen-Abstimmung.

Genau hier setzt die Wirkungsarchitektur an: erst die Wirkung, dann die Struktur. Sie ordnet nicht Behörden, sondern Beiträge – jede Stelle bleibt, was sie ist, und weiß zugleich, worauf sie einzahlt. Aus getrennten Zuständigkeiten, Informationen und Führungswegen wird eine durchgängige Kette.

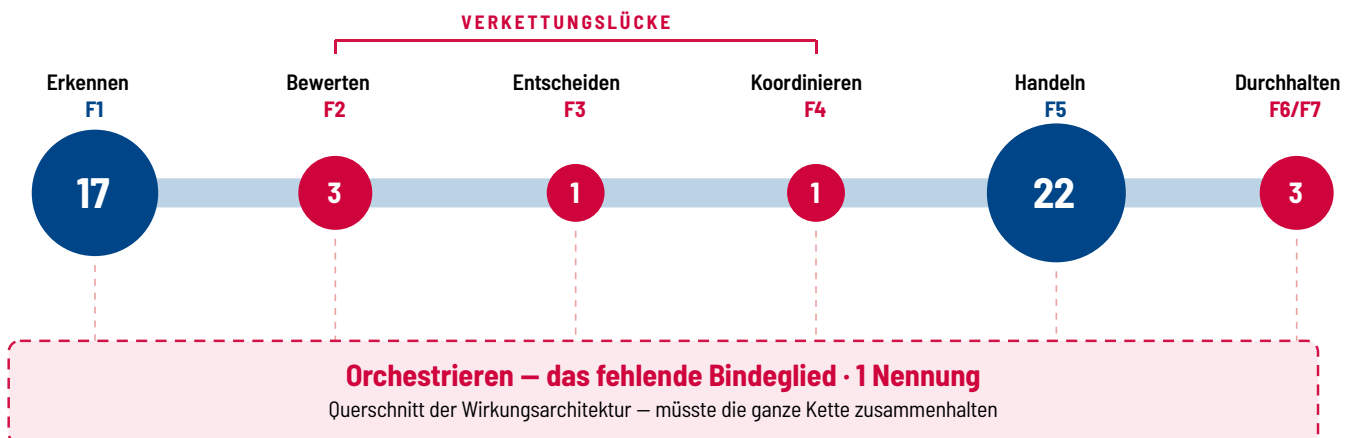
Damit ist die Verkettungslücke nicht nur benannt, sondern adressiert. Der folgende Abschnitt stellt die Fähigkeiten des Gesamtsystems vor und prüft ihren Reifegrad, bevor Kapitel 4 die Governance behandelt.

FÄHIGKEITSKETTE

Deutschland sieht und handelt – aber das Bindeglied fehlt.

Wirkung der Lösungen je Zielbild-Fähigkeit – stark an den Enden, dünn in der Mitte, leer im Querschnitt.

● besetzt – 10 Nennungen und mehr ● Leerstelle



Frage [26]: „Was hat die Lösung konkret geleistet?“ · 48 Wirkungsnennungen, primär codiert · GSÖ-Befragung unter Tech-Providern und Anwendern, N = 72

Abb. 3.5: GSÖ-Befragung und Maßnahmen-Datenbank GSÖ 2030

3.4 – DIE FÄHIGKEITEN

Sieben Fähigkeiten schließen die Handlungskette

Das Modell trennt das Was vom Wer. Es beschreibt zuerst die geforderte Leistung und ordnet danach den verantwortlichen Träger. Jede der sieben Fähigkeiten entsteht aus dem Zusammenspiel mehrerer Beteiligten, keine gehört einer Organisation allein.

Lage erkennen. Bei den Olympischen Spielen in Paris 2024 wurde der Luftraum an 18 Standorten überwacht, berichtet Axel Lips von Sopra Steria. Rund 3.000 genehmigte Drohnenflüge mussten laufend von unerlaubten unterschieden werden.

Lage bewerten. In Kopenhagen hört ein System Notrufe mit und erkennt an Stimme, Stichwörtern und Hintergrundgeräuschen Muster für einen Herz-Kreislauf-Stillstand – der Disponent bekommt den Hinweis, während das Gespräch läuft.

Entscheiden. Frankreich betreibt mit NexSIS eine einheitliche nationale Leitstellenplattform für Feuerwehr und Rettungsdienste, multikanalfähig und in Echtzeit.

Koordinieren. Das ukrainische System Delta integriert Aufklärungsdrohnen, Satellitenbilder, Sensoren und Meldungen verifizierter Zivilisten in eine gemeinsame Karte.

Wirksam handeln. Das LNG-Terminal Wilhelmshaven ging Ende 2022 nach 180 Tagen in Betrieb, berichtet Landrat Sven Ambrosy, weil Bund, Land, Kommune und Betreiber parallel statt nacheinander arbeiteten. Genehmigung, Bau und Beschaffung liefen gleichzeitig.

Resilienz sichern. Die ukrainische Energieversorgung verhinderte trotz massiver Angriffe einen landesweiten Blackout – durch Netzsegmentierung, manuelle Rückfallverfahren und isolierte Steuerungsanlagen.

Wiederherstellen und lernen. Als Ransomware 2021 das Netzwerk des Landkreises Anhalt-Bitterfeld verschlüsselte, blieb die Verwaltung nur handlungsfähig, weil Daten zuvor in ein getrenntes Rechenzentrum ausgelagert worden waren.

Die beiden am dünnsten besetzten Fähigkeiten sind genau die, an denen in Kapitel 2 die Ketten brachen: die Bewertung eines Signals und der Wiederanlauf danach.

EBENE 4

Was das System können muss, nicht wer es tut

F1 Lage erkennen & antizipieren Relevante Signale früh erkennen und Lageentwicklungen vorausschauend einschätzen.	F2 Lage bewerten & priorisieren Einordnen, Unsicherheiten transparent machen, Handlungsbedarfe priorisieren.	F3 Entscheiden & ausrichten Unter Zeitdruck entscheiden, Leitabsichten formulieren, Akteure wirkungsorientiert ausrichten.	F4 Koordinieren & führen Akteure, Ressourcen und Maßnahmen rollenbasiert koordinieren – ohne zentrale Detailsteuerung.
F5 Wirksam handeln Entscheidungen in überprüfbare Wirkung übersetzen und kritische Funktionen schützen.	F6 Resilienz sichern Auch unter anhaltender Störung handlungsfähig bleiben, Kaskaden begrenzen.	F7 Wiederherstellen & lernen Normalisierung beschleunigen und aus realen Lagen wie aus Übungen systematisch lernen.	

Abb. 3.6: Zielbild GSÖ 2030, Ebene 4

3.5 – DER BENCHMARK

Deutschland im Reifegrad-Check: weit abgeschlagen

Der Systemreifegrad-Benchmark vergleicht sechs Länder über zehn Dimensionen. Die Bundesrepublik kommt auf 14 von 30 Punkten und damit auf den niedrigsten Wert. Was das in Jahren bedeutet und wie andere Länder ihren Vorsprung aufgebaut haben, zeigen die folgenden Seiten.

Die Ukraine erreicht 22 von 30 Punkten, die Bundesrepublik kommt auf 14 und damit auf den niedrigsten Wert aller untersuchten Länder. Die Ursache liegt außerhalb dessen, worauf sich die öffentliche Debatte meist richtet.

Was der Benchmark misst. Zehn Dimensionen aus der Auswertung internationaler Sicherheitsstrategien, je Dimension drei Stufen: beschrieben, eingeführt, landesweit verbindlich. Gemessen wird der Aufbauzustand, nicht die Bewährung unter Last – ein formal vollständiges System kann im Ernstfall versagen. Die Werte der Referenzländer beruhen auf einer Dokumentenanalyse, für die Bundesrepublik kommen Befragung, Interviews und Lösungsdatenbank hinzu. Die zehn Dimensionen sind nicht die sieben Ebenen des Zielbilds. Seite 113 führt Verfahren und Grenzen aus.

Nur zwei der zehn Dimensionen betreffen Technik. Entscheidend ist die Verbindung vorhandener Mittel. Ein Land kann über ausgereifte Einzelprodukte verfügen und als Gesamtsystem dennoch zurückliegen. Der Verweis auf verfügbare Angebote widerlegt den Befund daher nicht.

Die Bundesrepublik erreicht in keiner Dimension den vollen Wert: sechs frühe Aufbauzustände, vier teilweise einsatzfähige, kein vollständiger Aufbau. Diese Verteilung findet sich in keinem anderen untersuchten Land. Die Niederlande und Finnland erzielen je sieben Höchstwerte, Schweden sechs.

Am schwächsten schneidet die Durchhaltefähigkeit mit zwei von sechs Punkten ab, gefolgt von der Steuerung mit vier von neun. Gerade diese beiden Blöcke entscheiden über die Handlungsfähigkeit in langen Lagen.

SYSTEMREIFEGRAD

Deutschland 14 von 30 Punkten – der niedrigste Wert im Vergleich

■ vollständig operativ ■ teilweise operativ ■ frühes Stadium

STEUERUNG

- 1 Governance & Orchestrierung**
Verbindliches ressortübergreifendes Mandat zur Steuerung über Bund, Länder und Sektoren.
- 2 Gemeinsames Lagebild**
Nationales, behörden- und sektorenübergreifendes Echtzeit-Lagebild mit Lieferpflicht.
- 3 Rechtliche Rahmenbedingungen**
Krisenrecht, Datenrechtsöffnungen, zivil-militärische Schnittstellen.

OPERATIVE WIRKUNG

- 4 Zivil-militärische Integration**
Operative Kopplung von BOS, Verwaltung und Bundeswehr: Lagebilder, Schnittstellen, Übergaben.
- 5 BOS-Interoperabilität**
Anschlussfähigkeit von Feuerwehr, Polizei, Rettung, THW über Länder- und Behördengrenzen.
- 6 KRITIS-Resilienz**
Verfügbarkeit kritischer Infrastrukturen und reziproke Anbindung an das staatliche Lagebild.

DURCHHALTEFÄHIGKEIT

- 7 Bevölkerungsvorsorge**
Akzeptanz, Mitwirkung und Eigenvorsorge der Bevölkerung als systemischer Wirkfaktor.
- 8 Wirtschaftliche Resilienz**
Mobilisierungs- und Durchhaltefähigkeit: Versorgung, Pool-Mechanismen, strategische Reserven.

ERMÖGLICHER

- 9 Digitales Rückgrat**
Technologische Trägerschicht D1 bis D8 für Lagebild, Kommunikation, Entscheidung, Recovery.
- 10 EDT-Integration**
Systematische Übernahme emergierender Technologien in Doktrin und Beschaffung.

Summe von 30 Punkten

	DE	NL	FI	SE	EE	UA
1	■	■	■	■	■	■
2	■	■	■	■	■	■
3	■	■	■	■	■	■
4	■	■	■	■	■	■
5	■	■	■	■	■	■
6	■	■	■	■	■	■
7	■	■	■	■	■	■
8	■	■	■	■	■	■
9	■	■	■	■	■	■
10	■	■	■	■	■	■
Summe	14	27	27	26	25	22

Abb. 3.7: Systemreifegrad-Benchmark

Mehr als zehn Jahre – der Rückstand lässt sich datieren

Für jede schwache Dimension dokumentiert der **Systemreifegrad-Benchmark**, wann Referenzländer den heute in Deutschland angestrebten Stand erreichen. Unabhängig davon bestätigen die Interviews die gleichen Lücken.

Beim Governance-Mandat beträgt der Abstand 13 Jahre. Finnland hält den Standard seit 2012, in der Bundesrepublik fehlt ein ressortübergreifendes Mandat. Benedikt Meng von infodas beschreibt, was an seine Stelle tritt: eine Folienschlacht, in der ein Polizeihauptkommissar den Gefechtsstand einer Heimatschutzkompanie aufsucht und zwischen den Organisationen übersetzen muss.

Beim gemeinsamen Lagebild sind es mehr als fünfzehn Jahre. In den Niederlanden ist es seit über einem Jahrzehnt vollständig einsatzfähig und gesetzlich verankert. Das Gemeinsame Kompetenzzentrum Bevölkerungsschutz erreicht diesen Stand frühestens 2028, eine Anschlusspflicht der Länder ist auch dann nicht vorgesehen.



„Jeder hat sein Lagebild, aber die Vernetzung der Lagebilder ist noch nicht umgesetzt.“

Bernd Reitmeier • Leitung Account Management
BWI, Bechtle

Für die zivil-militärische Integration lässt sich kein Zeitpunkt angeben. Finnland, Schweden und die Ukraine erzielen den Höchstwert, die Bundesrepublik einen von drei Punkten. Diese kritischste Einzeldimension bietet keinen ausländischen Aufbaupfad, der sich einfach übertragen ließe. Martha Klare von der Universität der Bundeswehr beschreibt an der Schnittstelle ein gegenseitiges Warten: Beide Seiten erwarten den ersten Schritt der jeweils anderen.

Bei der Bevölkerungsvorsorge beträgt der Abstand zehn bis 20 Jahre. Finnland verankert sie seit zwei Jahrzehnten in Bildung und Verwaltung, Schweden verteilte 2024 sein Notfallhandbuch an alle 4,8 Millionen Haushalte. Die deutsche Selbstschutzkampagne startete 2026. Frank Weber nennt die Voraussetzung: Die Bevölkerung müsse wieder verstehen, dass der Staat nicht wie ein Rettungsdienst binnen neun Minuten jede Katastrophe abwenden kann.

Bei der wirtschaftlichen Resilienz sind es mehr als zehn Jahre. Finnlands Versorgungssicherheitsagentur steuert seit Jahren branchenspezifische Arbeitskreise, sogenannte Sektorpools, in denen Betreiber verbindlich Kapazitätsdaten liefern. Ein vergleichbares Verfahren fehlt hierzulande. Christian Growitsch von der HICCE fordert, kritische Produktionskapazitäten als Sicherheitsthema zu behandeln.

Eine Dimension fällt aus dem Vergleich heraus. Bei der Integration neuer Technologien erreicht außer der Ukraine kein Land mehr als zwei Punkte. Hier beginnt die Bundesrepublik auf dem gleichen Stand wie die übrigen Referenzländer.

Keiner dieser Rückstände ist neu. Jeder hat einen Anfang, den andere Länder vor Jahren gesetzt haben.

Politische Beschlüsse begründen den Vorsprung

In allen Referenzländern lässt sich der Ausgangspunkt des Aufbaus datieren. Der formale Auftrag ging der späteren Fähigkeit jeweils voraus. Für jede deutsche Lücke findet sich ein solcher Anfang.

Governance: In Schweden genügte ein Mandat. Zum 1. Januar 2026 erhielt die Behörde für Gesellschaftsschutz und Bereitschaft (MSB) den Leitungs- und Koordinierungsauftrag für das zivile Verteidigungswesen, daneben entstand ein Ministeramt. Zusätzliche Mittel oder ein neues Gesetzeswerk waren nicht nötig. Der entscheidende Schritt war das Mandat. In der Erhebung ist Schweden das am häufigsten genannte Vorbild.

Lagebild: Die Niederlande machten die Nutzung zur Pflicht. Das Gesetz über die Sicherheitsregionen schuf 25 regionale Wirkungsräume mit einer gemeinsamen Plattform für Feuerwehr, Polizei, Gesundheitsdienste und Gemeinden. Ihre Nutzung ist verpflichtend. Übertragbar ist diese Konstruktionsentscheidung, nicht das Gesamtsystem.

Durchhaltefähigkeit: Finnland verbindet das seit 2003 bestehende Modell umfassender Sicherheit mit einem Mandat und jährlicher Rechenschaft gegenüber der Regierung. Branchenspezifische Arbeitskreise verpflichten Betreiber zur Lieferung von Kapazitätsdaten und geben ihnen im Gegenzug Planungssicherheit.

Zwei Fälle verlangen eine eigene Einordnung. Estland legte mit X-Road eine Vermittlungsschicht zwischen bestehende Register und vermied damit den Austausch der gesamten Dateninfrastruktur. Die Ukraine ist der einzige unter Last erprobte Fall. Ihre im Krieg entstandene Architektur lässt sich nicht als Friedensmodell kopieren.

Zwei Einschränkungen bleiben. Estland, Finnland und Schweden leben mit einer unmittelbaren Bedrohungswahrnehmung, die einen Teil ihres Vorsprungs erklärt. Und die deutsche Datengrundlage ist dünn: Das Sendai-Rahmenwerk der Vereinten Nationen für Katastrophenvorsorge, 2015 bis 2030, verlangt eine systematische Erfassung von Schäden und Ausfällen. Deutschland liefert dafür bislang keine belastbaren Daten.



„Wir können davon nichts berichten – wir sind da ein bisschen im Blindflug.“

Dr. Benni Thiebes • Geschäftsführer, DKKV

Der Rückstand ist kein Technikproblem, sondern eine Frage unterlassener Entscheidungen. Bleibt die Frage, woran ein belastbarer Beschluss zu erkennen ist. Der letzte Abschnitt beantwortet sie.



„Ich wünsche mir die Vereinigung des Guten aus beiden Welten – den niederländischen Pragmatismus, gepaart mit der Ehrenamtlichkeit, der Helferkultur und der kommunalen Selbstverantwortung, die wir haben.“

Sven Ambrosy • Landrat, Landkreis Friesland

3.6 – DER MASSSTAB

Sechs Fragen trennen Auftrag von Absicht

Ein politischer Beschluss ist noch kein Auftrag. Sechs Fragen entscheiden darüber, ob eine Maßnahme trägt – gestellt von Menschen, die Lagen geführt haben. Bleibt eine davon offen, bleibt es bei der Absicht.

Ist das Zielniveau festgelegt? Ohne einen vereinbarten Sollzustand lässt sich weder Erfolg noch Rückstand feststellen. Marlis Cremer von den DRK-Kreisverbänden Düren und Jülich stellt die Frage, die vor allen anderen kommt.



„Wie gut wollen wir denn sein? Solange wir uns nicht darauf verständigen, kann ich gar nicht sagen, ob wir an den Grenzen sind, weit darunter oder weit darüber.“

Marlis Cremer • Präsidentin,
DRK-Kreisverbände Düren und Jülich

Wirkt die Maßnahme vor dem Ereignis oder erst danach? Christian Hummert von der Cyberagentur hält den Leitbegriff Resilienz für zu eng. Abwehr, Erholung und anschließende Verbesserung setzten voraus, den ersten Treffer auszuhalten. Ergänzend brauche es das Vorausschauende, das er Vigilanz nennt. Ein Instrument, das erst nach dem Treffer greift, bleibt zweite Wahl.

Trennt sie das Besondere vom Üblichen? Kai Drücker von conet leitet aus der Marktbeobachtung ab, dass sich nicht alles schützen lässt. Nötig seien Eindämmungspläne und eine Klassifizierung: welche Daten und Infrastrukturen wie schützenswert sind. Manches lasse sich besonders schützen, anderes bewusst schneller reparieren – ökonomisch oft sinnvoller, als überall dasselbe Schutzniveau anzustreben.

Ist der Wiederanlauf mitgeplant? Armin Schaus vom Operativen Führungskommando beschreibt den Wechsel von der Resistenz zur Resilienz. Früher habe man auf ein Netz gesetzt, in das niemand eindringen könne. Heute müsse man mit dem Angriff rechnen und einen Plan für die schnelle Rückkehr in die normalen Geschäftsprozesse bereithalten.

Reicht die Durchhaltezeit bis zur Rückkehr in den Normalbetrieb?

Kai Hoberg von der Kühne Logistics University nennt zwei Kennzahlen aus dem Lieferkettenmanagement: Die Überlebensdauer beschreibt, wie lange ein Betrieb mit vorhandenen Beständen auskommt. Die Erholungsdauer, wie schnell seine Kapazität zurückkehrt. Der erste Wert muss größer sein als der zweite. Für einen einzelnen Betrieb klingt das selbstverständlich, im Gesamtbild wird es selten erreicht.

Ist der Preis der Resilienz benannt? Christian Growitsch vom HIICCE beschreibt Überkapazitäten, Vorräte und Redundanzen als betriebswirtschaftlich ineffiziente, zugleich wirksame Vorsorge gegen physische Nichtverfügbarkeit. Steigen die Folgen einer Unterbrechung bis zur Gefahr für Leib und Leben, lohnt sich diese Versicherung. Was heute Redundanz heißt, war früher selbstverständliche Lagerhaltung.



„Resilienz hat Kosten, und Resilienz schafft Werte.“

Dr. Christian Growitsch • Geschäftsführer, HIICCE

Die Kapitel 4 bis 7 entwickeln daraus den Handlungsweg: die Governance, die das Mandat trägt, das digitale Rückgrat, das die Kopplung ermöglicht, die Marktbeiträge, die auf das Zielbild einzahlen, und die erprobten Schritte zur Umsetzung.

Eine Absicht wird erst dann zum Auftrag, wenn alle sechs Fragen beantwortet sind.

04

Governance first

**Ohne Orchestrierung
keine Wirkung**

4.0 – DIE ROLLEN

Viele Verantwortliche, keine Führung



Die deutsche Sicherheitsarchitektur kennt Verantwortliche für fast jeden Ausschnitt. Governance, also die Regeln für Führung, Verantwortung und Durchgriff, entscheidet darüber, ob aus diesen Ausschnitten eine gemeinsame Leitabsicht entsteht.

Sechs Rollen tragen das gesamtstaatliche Sicherheitsgefüge, von der strategischen Führung bis zum Wiederanlauf. Vier sind institutionell besetzt. Offen bleiben die verbindliche operative Koordination und die Verdichtung zum gemeinsamen Lagebild. Die Schwelle liegt dort, wo mehrere korrekte Zuständigkeiten gleichzeitig Führung brauchen. → [4.1](#)

Der Rechtsrahmen setzt drei gewollte Grenzen: Mischverwaltung, Trennungsgebot und die engen Voraussetzungen für den Einsatz der Streitkräfte im Inland. Der Zeitverlust entsteht häufig schon davor, solange die Lage rechtlich noch eingeordnet wird. Verfassungsgrenzen und Auslegungsprobleme sind zweierlei. → [4.2](#)

Regulierung erfasst Betreiber, Anlagen und Meldepflichten. Kaskaden entstehen jedoch zwischen ihnen, während Rückmeldungen aus dem Staat an Unternehmen langsam, eingestuft oder gar nicht zurücklaufen. Diese Reziprozitätslücke reicht vom KRITIS-Rahmen bis zur konkreten Meldekette. → [4.3](#)

Seit 2026 gibt es institutionelle Orte für gesamtstaatliche Führung: den Nationalen Sicherheitsrat und einen entstehenden Steuerungstab für die zivile Verteidigung. Ihre Wirkung hängt an Mandat, Rang, Personal und Durchgriff. Aus Koordination wird erst dann verbindliche Orchestrierung. → [4.4](#)

Drei Bausteine verdichten die Interviews zu einer Führungsarchitektur: ein Sicherheitsrat mit Weisungskompetenz, ein ziviler Operationsplan und eine mandatierte Stelle für die Lagebildverdichtung. Zusammen ergeben sie eine Kette vom Lagebild bis zum Auftrag. → [4.5](#)

Im Bündnisfall kehrt sich die gewohnte Unterstützungsrichtung um. Die Bundeswehr braucht zivile Korridore, Logistik, Sanitätskapazitäten und Unternehmen. CIMIC Quadriga 2026 zeigt, wie diese Schnittstelle unter realen Rollen geübt werden kann. Governance reicht damit über den Ressortverbund hinaus in die Gesamtverteidigung. → [4.6](#)

Führung wird konkret, sobald Ressourcen knapp werden. Strom, Treibstoff, Brücken, Transportkapazitäten und Lieferketten brauchen eine vorab geklärte Reihenfolge, damit Systemrelevanz im Ernstfall handlungsleitend wird. Priorisierung ist die operative Form staatlicher Souveränität. → [4.7](#)

Am Ende steht das Mandat. Acht institutionelle Entscheidungen bündeln, was dieses Kapitel aus Recht, Regulierung, Führungsstruktur, Versorgung und Gesamtverteidigung ableitet. Governance wird damit zum Arbeitsauftrag bis 2030. → [4.8](#)

4.1 – DAS GRUNDPROBLEM

Zuständigkeit klärt Haftung, nicht Führung

Überschreitet eine Lage die Grenze eines Landkreises, ist auf dem Papier geklärt, wer sie führt und haftet. Offen bleibt, wer die Akteure zusammenführt, die von diesem Moment an gleichzeitig handeln müssen.

Das deutsche Sicherheitsgefüge ordnet Verantwortung eindeutig: **Aufgaben haben Träger, Träger haben Rechtsgrundlagen und Kontrollinstanzen.** Diese Ordnung heißt Föderalismus, eine Gründungsentscheidung von 1949 gegen die Bündelung von Macht in wenigen Händen. Sie sorgt für zurechenbare Eingriffe und parlamentarisch überprüfbare Entscheidungen. Wer sie lockert, gewinnt keine Geschwindigkeit und verliert Rechenschaft. Ihre Grenze zeigt sich bei einer Lage, die mehrere Träger zugleich betrifft. Dann arbeitet jeder korrekt in seinem Ausschnitt, während das Ganze ohne Führung bleibt.

36

von 100 Punkten

Eine geklärte Verantwortung erzeugt noch keine abgestimmte Handlung. Wer zuständig ist, weiß, was er zu tun hat. Er weiß nicht, was die anderen tun, in welcher Reihenfolge und mit welcher Priorität. In einer Lage, die Energieversorgung, Verkehr, Gesundheitswesen und Kommunikation zugleich trifft, entstehen mehrere richtige Teilentscheidungen und kein gemeinsames Ziel. Der Fehler liegt in keiner dieser Entscheidungen. Er liegt darin, dass niemand sie aufeinander bezieht.

Handlungsfähigkeits-Index

GSÖ-Befragung unter Tech-Providern und Anwendern, N=72

Koordination stellt Einvernehmen her, verbindliche Koordination erzeugt gemeinsame Wirkung. Sie bringt Beteiligte an einen Tisch, gleicht Absichten ab und endet beim Dissens. An dieser Stelle muss eine benannte Stelle die Leitabsicht formulieren, Schutzgüter priorisieren und entscheiden. Dafür braucht sie ein Mandat. Fehlt es, bleibt das Treffen ein Gesprächsformat. Eine neue Behörde ist dafür unnötig, entscheidend ist die Befugnis, im Ernstfall die Reihenfolge zu bestimmen.



„Was passiert, wenn wir eben nicht eine regional begrenzte Lage haben, sondern eine Lage, bei der eine länderübergreifende und ressortübergreifende Koordination erforderlich ist?“

Wolfgang Gäbelein • Generalmajor a.D. und Vorsitzender, DWT

Solange eine Lage räumlich begrenzt bleibt, trägt das System. Eine Landesregierung übernimmt, Amtshilfe läuft an, die Zuordnung ist eindeutig. Jenseits dieser Grenze beansprucht das Bundesministerium des Innern (BMI) zwar, Rahmen zu setzen, hat aber nie formuliert, die Länder koordinieren zu wollen. Daraus entsteht eine weiche Flanke.

Sechzehn Systeme des Katastrophenschutzes sind eine Folge der grundgesetzlichen Zuständigkeit der Länder. Christian Miller von der Feuerwehr Köln nennt die Konsequenz: 16 Rechtsgrundlagen, 16 Begriffswelten. Das ist Verfassungsfolge, nicht Versäumnis. Bayern verlangt mit der Erklärung des Katastrophenfalls einen förmlichen Rechtskreiswechsel. Nordrhein-Westfalen kommt ohne diese Feststellung aus. Unterschiedliche Rechtsgrundlagen und Begriffe erschweren bereits den Vergleich einsatztaktischer Werte über Ländergrenzen hinweg. Eine Vereinheitlichung würde das Grundgesetz berühren und den entscheidenden Übergang noch immer nicht regeln.

Wirkung entsteht nicht dort, wo Verantwortung endet, sondern dort, wo jemand sie zusammenführt.

Die Kette reißt an der Schwelle zwischen Zuständigkeiten

Bundesweit fehlt eine verbindliche Definition dieses Übergangs.

Norbert Ahrend von Arvato Systems bezeichnet den Wechsel von der kommunalen zur Landesebene als die am schwersten zu schließende Lücke. Als ungeschriebene Regel gilt: Ab drei betroffenen Landkreisen übernimmt das Land. Festgeschrieben ist das nirgends. Der typische Ablauf führt vom Landkreis über den Abteilungsleiter und den Staatssekretär bis zum Minister. So kann ein Tag vergehen, bevor eine koordinierende Entscheidung fällt.

Gerald Funke vom Unterstützungskommando der Bundeswehr

betrachtet den Übergang von der anderen Seite. Die Bundeswehr könne aus einer bundesweiten Gesamtsicht planen, wolle der Bundesinnenminister handeln, müsse er sich mit 16 Landesinnenministern abstimmen, die eigene Zuständigkeiten und Haushalte haben. Ein militärischer Befehlshaber beschreibt damit die eigene Lage als den einfacheren Fall.

Paul Höller aus dem nordrhein-westfälischen Wirtschaftsministerium hält dem Föderalismus zugute, dass er die Reaktionszeit gegenüber zentralistisch organisierten Staaten verkürzt: Der Landrat ruft den Kreisbrandmeister direkt an, statt auf eine ferne Hauptstadt zu warten. Schwierig wird es erst, wenn ein Ereignis eine Größenordnung

erreicht, der einzelne Länderstrukturen nicht gewachsen sind.

Dass die Kette dennoch meist hält, hat einen Preis.

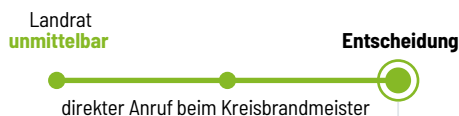
Tobias Schönherr von der Bundespolizei schildert Momente, in denen Struktur durch persönliche Risikobereitschaft ersetzt wird: Einzelne entscheiden, jetzt loszufliegen, und nehmen den Ärger hinterher in Kauf. Der Befund begrenzt sich selbst. Martin Zeidler vom BBK hält fest, dass Deutschland komplexe Lagen dank großem Improvisationstalent meist gut bewältigt und der Bruch nicht in der Tagesarbeit liegt. In den Gesprächen aus dem kommunalen Bereich kommt der Zusatz: In der normalen Katastrophe ist die Zuständigkeit klar geregelt, samt Weisungsrechten. Was fehlt, ist die Regelung des Übergangs oberhalb der Landesebene. Ob der Rechtsrahmen diesen Übergang verhindert oder ob er nur nicht genutzt wird, ist die Frage des nächsten Abschnitts.

**Wenn es darauf ankommt, funktioniert es
– weil Einzelne Verantwortung übernehmen
und Vorgaben beiseiteschieben.**

ESKALATION

Minuten, Stunden oder Tage – je nachdem, wer entscheiden darf

INNERHALB EINER EBENE



DIE SCHWELLE

Nirgends bundesweit definiert.

Ungeschriebene Regel: drei betroffene Landkreise.

ÜBER DIE EBENENGRENZE



Abb. 4.2: Tiefeninterviews GSÖ 2030

4.2 – DER RECHTSRAHMEN

Das Recht erlaubt mehr, als Deutschland nutzt

Neue Gesetze gelten schnell als Antwort auf jede Lücke im Sicherheitsgefüge. Der Bestand weist in eine andere Richtung. Thomas Hambach vom Landeskommmando Bayern zählt rund 15 Vorsorge- und Sicherstellungsgesetze, die sämtlich in Kraft sind und derzeit überarbeitet werden. Veraltet oder ungeklärt sind vor allem ihr Auslösezeitpunkt und ihr Zusammenspiel.

Die Lage, in der sie greifen müssten, lässt sich schwer benennen.

Armin Fleischmann bringt sie auf eine Formel: Deutschland sei nicht mehr im Frieden, aber auch nicht im Krieg. Cyberangriffe auf die deutsche Wirtschaft fänden in großer Zahl statt, das sei kein Frieden mehr. Zugleich gebe es keine Kriegserklärung und damit keinen Spannungsfall, sodass die Krisengesetzgebung nicht greife.

Der Rechtsrahmen setzt drei gewollte Grenzen. Das Verbot der Mischverwaltung trennt die Verwaltungszuständigkeiten von Bund und Ländern. Das Trennungsgebot begrenzt die Verknüpfung von Polizei und Nachrichtendiensten. Artikel 87a des Grundgesetzes setzt dem Einsatz der Streitkräfte im Inland außerhalb der ausdrücklich vorgesehenen Fälle enge Grenzen. Die Interviews behandeln diese Prinzipien als gesetzten Rahmen. Zeitverlust entsteht früher: Solange eine Lage noch als Unfall, Straftat, Cyberoperation oder staatlich gesteuerter Angriff eingeordnet wird, bleibt offen, welcher Rechtskreis greift und wer handeln darf.

Der Nationale Sicherheitsrat hat am 8. Juni 2026 eine Überprüfung dieser Rechtsgrundlagen beschlossen. Damit steht ein Verfahren offen, in das Krisendatenaustausch und Betreiberpflichten eingespeist werden können.

Der Gesetzgeber hat inzwischen mehrere Befugnisse erweitert. Anfang 2026 wurden das Gesetz über den unmittelbaren Zwang der Bundeswehr und das Luftsicherheitsgesetz geändert. Der neue Paragraf 15a erlaubt den Streitkräften als letztes Mittel Waffengewalt gegen unbemannte Fluggeräte und konkretisiert die Amtshilfe nach Artikel 35 des Grundgesetzes. Seit Dezember 2025 bündelt das Gemeinsame Drohnenabwehrzentrum in Berlin Kräfte von Bund und Ländern. Am 10. Juli 2026 nahm der Bundestag die Novelle des Bundespolizeigesetzes an. Gemeinsame Übungen und Verwaltungsvereinbarungen zwischen Bund und Ländern sind ohne weitere Rechtsgrundlage möglich. Der Engpass wandert damit von der Ermächtigung zur gemeinsamen Anwendung.

Vier Akteure teilen sich den Luftraumschutz im Inland: Bundespolizei, Landespolizeien, Flugsicherung und Bundeswehr. Ihre Befugnisse sind seit 2026 erweitert, ein gemeinsames Luftlagebild in Echtzeit fehlt weiterhin. Am 5. August 2026 wurde am Flughafen Leipzig/Halle eine Drohne mit verdächtiger Vorrichtung gefunden. Die Bundespolizei sicherte das Fluggerät, der Generalbundesanwalt übernahm die Ermittlungen. Zwei Tage zuvor hatte secunet-Vorstand Marc-Julian Siewert in einem Interview mit The Pioneer die asymmetrische Logik der Cyberabwehr beschrieben: Ein Angreifer sucht eine Lücke, die Verteidigung muss alle schließen. Diese Logik gilt auch am Flughafen. Der Angreifer braucht eine blinde Stelle. Die Verteidigung muss Detektion, Lagebild, Freigabe und Wirkung lückenlos verbinden. So wird die einzelne Schwachstelle zur Verkettungslücke.

Offen bleibt die Auslegung des Trennungsgrundsatzes. Der historisch begründete Schnitt zwischen innerer und äußerer Sicherheit lässt sich unter der heutigen Bedrohungslage, besonders im Cyberraum, kaum widerspruchsfrei anwenden. Dasselbe gilt für den föderalen Datenschutz bei Breitbanddiensten und für die Zurechnung von Cyberangriffen: Beide sind nicht unregelt, sondern unterschiedlich auslegbar. Die nötige Debatte betrifft daher den Gebrauch der vorhandenen Normen.

Neue Befugnisse ersetzen kein gemeinsames Lagebild

Mit neuen Eingriffsbefugnissen muss die Kontrolle wachsen.

Automatisierte Gefahrenerkennung und biometrische Echtzeitdetektion sind Anwendungen künstlicher Intelligenz im Sicherheitsbereich. Sie fallen unter Anhang III der Verordnung über künstliche Intelligenz, die Hochrisikopflichten wurden durch den Digital Omnibus auf Dezember 2027 verschoben. Damit entsteht die Befugnis vor der Aufsichtspflicht. Zuständigkeit sichert Haftung, Finanzierung und parlamentarische Kontrolle. Schnellere Freigaben müssen diese drei Funktionen erhalten. Christian Hummert von der Cyberagentur beschreibt die frühere Rechtslage anhand der Drohnenüberflüge: Zuständig sei eine lokale Polizeidirektion ohne geeignete Mittel gewesen, während die Bundeswehr nicht eingreifen durfte.



„Wenn es reicht, eine Landesgrenze zu überfliegen, um aus der Zuständigkeit zu sein, sind wir auf Dauer ein Papiertiger.“

Dr. Bernd Calaminus • Head of Business Resilience, [EnBW](#)

Die Befugnis ist geklärt, die Verfügbarkeit nicht. Paul Höller aus dem nordrhein-westfälischen Wirtschaftsministerium meint keine Waffensysteme auf dem Dach, er meint digitale Mittel: Störsender, das Übernehmen der Steuerung, im Zweifel das Abfangen mit einer Netzdrohne. Die Abwehrkräfte der Landespolizei sind zentral organisiert und vorrangig für Großereignisse vorgesehen, wird eine Drohne andernorts gesichtet, ist sie längst weg, bis die Kräfte eintreffen. Von

der Anbieterseite wird das bestätigt: Betreiber kritischer Infrastrukturen dürfen im nahen Luftraum über dem eigenen Gelände nicht wirken, obwohl es technologisch möglich wäre. Höllers Leitfrage lautet schlicht: Wer darf es tun?

Leonard Wessendorff, Jurist von Haus aus, verschiebt die Frage. Das Hauptargument in der Debatte über den Abschuss einer Drohne sei, auf wessen Kopf die Trümmerteile fallen. Deutschland sei sehr risikoavers. Die Grenze liegt damit an mancher Stelle in der Bereitschaft, das Recht anzuwenden.

Zwei Öffnungen bleiben unerledigt. Die erste ist der Selbstschutz von Betreibern über dem eigenen Gelände. Die zweite ist die Schwelle, an der die Verantwortung von der kommunalen auf die Landes- und weiter auf die Bundesebene übergeht, sie ist in keinem Gesetz beziffert.

Alles Übrige, was in den Gesprächen als Rechtsproblem erschien, ist geregelt oder eine Frage der Auslegung. Damit wandert der Engpass zu den Regelwerken, die Betreiber und Behörden verbinden: Erfassen sie die Verkettung von Störungen überhaupt?

BEFUGNISSE

Das Recht erlaubt mehr, als Deutschland nutzt

MÖGLICH

geltendes Recht trägt

- Amtshilfe nach Artikel 35 Grundgesetz
- § 15a Luftsicherheitsgesetz — Befugnisse gegen unbemannte Fluggeräte
- Drohnenabwehr durch die Bundespolizei nach der Novelle vom 10. Juli 2026
- Gemeinsame Übungen und Verwaltungsvereinbarungen

AUSLEGUNGSBEDÜRFTIG

Praxis bleibt unsicher

- Datenaustausch unter dem Trennungsgrundsatz
- Föderaler Datenschutz bei Breitbanddiensten
- Attribution im Cyberraum

ÖFFNUNG NÖTIG

Regelungslücke

- Selbstschutz von Betreibern im nahen Luftraum über dem eigenen Gelände
- Verbindliche Schwelle für den Verantwortungsübergang zwischen den Ebenen
- Aufsicht über KI-gestützte Gefahrenerkennung
- Gemeinsames Luftlagebild in Echtzeit

Abb. 4.3: Rechts- und Governance-Rahmen GSÖ 2030

4.3 – DIE REGULIERUNG

Meldepflicht ohne Rückkanal

Mit Registrierungspflichten, Meldewegen und Mindeststandards zieht das KRITIS-Dachgesetz einen Kreis um die staatlich anerkannte kritische Infrastruktur. Es ordnet die Beziehung zwischen Staat und individuellem Betreiber. Die Verbindungen der Betreiber untereinander bleiben außerhalb dieses Kreises.

Lagen eskalieren, sobald ein Ausfall den nächsten auslöst. Das Gesetz erfasst Objekte und lässt ihre Abhängigkeiten offen. Hanno Friedrich von der Kühne Logistics University zeigt das am Verkehr: Erfasst wird die Infrastruktur, während Logistikunternehmen und Güterverkehr außerhalb bleiben. Auch die Schwelle der NIS-2-Richtlinie, der europäischen Vorgabe für Cybersicherheit in kritischen und wichtigen Einrichtungen, sei für den Lebensmittelsektor zu grob: Ab einer halben Million Betroffener greift sie. Dort könne bereits ein kleines Unternehmen weitreichende Kettenwirkungen auslösen.

Auch in der Versorgung wirkt diese Definitionsgrenze. Michael Kreinest von der BG Klinik Ludwigshafen verweist auf Wohngemeinschaften beatmungspflichtiger Menschen ohne Notstromversorgung: Sie zählen nicht zur kritischen Infrastruktur und sind nicht meldepflichtig. Mit der Umsetzung der Richtlinie wächst der Kreis der erfassten Unternehmen von rund 1.200 registrierten Betreibern auf schätzungsweise 33.000. Sven Hallbauer von der EWERK Group nennt diese Zahl für die jüngste Verschärfung. Mehr Erfasste bedeuten allerdings nicht mehr Verbindung. Für große Betreiber ist die Mehrfachmeldung stemmbar, für Mittelständler nicht.

Eine Meldepflicht ohne Rückkanal senkt die Bereitschaft zur Weitergabe. Benedikt Meng von infodas nennt das die Reziprozitätslücke: Das Gesetz regle vor allem die Pflichten des Betreibers gegenüber dem Staat, lasse dessen Gegenleistung jedoch offen. Armin Schaus vom Operativen Führungskommando der Bundeswehr erklärt, warum: Sobald eine Meldung Verpflichtungen auslöst, erhält sie den Stempel Verschlusssache und wird für Unternehmen unbrauchbar.

Die Einstufung ist nicht der einzige Grund. Ein Teil der Erkenntnisse unterliegt zugesagter Vertraulichkeit, andere Meldungen stammen aus internationalen Quellen, deren Weitergabe an Vertrauensregeln gebunden ist. Hinzu kommt die organisatorische Trennung. Jeder dieser Gründe ist nachvollziehbar. Zusammen ergeben sie ein System, das Informationen einsammelt und keine zurückgibt.

In einem Haus wurde daraus eine Konsequenz. Nach einem Anschlag forderte am selben Tag eine Behörde die Ergebnisse aus Audits von Angriffserkennungssystemen samt vollständigem Netzplan, während eine andere dringend riet, genau solche Informationen nicht mehr herauszugeben. Seither werden nur noch generische Angaben weitergereicht. Der Staat fordert Angriffsdaten und warnt zugleich davor, sie zu teilen.

Wie viel Zeit verloren gehen kann, zeigt ein Fall aus dem Energiesektor. Nach Angriffen auf Windkraftanlagen in Polen erhielt ein deutscher Betreiber die Information zunächst von niederländischen Behörden. Deutsche Stellen übergaben dieselbe Information zwei Wochen später in einem eigenen Termin. Der Betreiber war längst gewarnt. Für andere Adressaten waren diese zwei Wochen verloren.

Keine dieser Lücken lässt sich durch eine weitere Meldepflicht schließen. Gebraucht wird eine Stelle, die drei Dinge tut: den Rückkanal betreiben, die Verbindungen zwischen den Betreibern erfassen und festlegen, was zuerst geschützt wird. Ob es sie gibt, ist die Frage des nächsten Abschnitts.

4.4 – DIE ORCHESTRIERUNG

Ein Sicherheitsrat ohne Durchgriffsrechte

Seit 2026 existieren erstmals Strukturen für die gesamtstaatliche Führung. Der Nationale Sicherheitsrat arbeitet seit Januar 2026 und tagt regelmäßig, zuletzt im September nach einem hybriden Anschlag in Leipzig. Das Bundesinnenministerium richtet einen Steuerungsstab für die zivile Verteidigung ein, den Fachleute als ziviles Gegenstück zum Operativen Führungskommando verstehen. Die Rolle hat damit einen institutionellen Ort.

Der Engpass liegt nun in der Ausstattung dieser Stellen. Verbindliche Führung verlangt Weisungsrecht, Rang und Personal. Ein Referat für das integrierte Lagebild mit unbesetzten Stellen, eine Leitung ohne Staatssekretärsrang und fehlender Durchgriff in die Ressorts ergeben eine Struktur, die Entscheidungen vorbereiten, aber kaum durchsetzen kann.

Die meisten Interviewpartner verorten die Rolle am selben Ort. Peter Holm vom Bundesverband Güterkraftverkehr argumentiert vom Grundgesetz her: Wer die Richtlinien der Politik bestimmt, ist der Bundeskanzler. Damit sei das Kanzleramt der natürliche Orchestrator. Dagegen steht ein Hoheitsprinzip, in dem jedes Ressort sein Thema verteidigt.

Auch die Bundeswehr kennt diese Lücke. Fragt man die Teilstreitkräfte, beansprucht jede die Führung für sich. Sachlich läge die Antwort beim Generalinspekteur, doch die Debatte um einen Generalstab will niemand führen.

Ein Konsens ist das nicht. Thomas Scholle von der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) hält Grundorganisation und Governance ausdrücklich für gut. Ein weiterer Gesprächspartner verschiebt den Fokus: Schnelle Umsetzung sei wichtiger als die Auswahl des zuständigen Organs.



„Ich bin nicht sicher, ob wir ein Verantwortungsproblem haben – ich glaube, wir haben ein Verantwortungsabgrenzungsproblem.“

Gerald Funke • Generalleutnant, Befehlshaber Unterstützungskommando, Bundeswehr

VERANTWORTUNG

Sechs Rollen, zwei offene Mandate

SYSTEMROLLE	WER DIE ROLLE HEUTE WAHRNIMMT	BEFUND
R1 Strategische Führung	Nationaler Sicherheitsrat seit Januar 2026 · Bundeskanzleramt · Ressortkrisenstäbe · Länderkrisenstäbe	Mehrfach besetzt – ohne verbindliche Eskalationslogik zwischen den Besetzungen.
R2 Operative Koordination	BBK mit Gemeinsamem Melde- und Lagezentrum · Steuerungsstab Kommando Zivile Verteidigung im Aufbau · Landeskommandos der Bundeswehr	Ohne Mandat, ohne Lagebild-Autorität.
R3 Behörden und Einsatzkräfte	Polizeien von Bund und Ländern · Feuerwehren · THW · Rettungsdienste · Leitstellen	Operativ tragfähig – aber in sechzehn Landessystemen mit unterschiedlichen Rechtsgrundlagen.
R4 Infrastrukturbetreiber	KRITIS-Betreiber in Energie, Wasser, Telekommunikation, Verkehr und Gesundheit	Reguliert – aber ohne Priorisierungsregel für den Ernstfall.
R5 Lagebild und Datenaustausch	BBK · BSI · BKA · Cyberagentur · Gemeinsames Terrorismusabwehrzentrum · Zentrum zur Abwehr hybrider Bedrohungen	Kein Mandat zur Lagebildverdichtung. Kritischste Lücke.
R6 Durchhaltefähigkeit & Wiederanlauf	Hilfsorganisationen · rund 1,76 Millionen Ehrenamtliche · Länder und Kommunen · Bevölkerung	Stark aufgestellt – die Interoperabilität zwischen den Organisationen fehlt.

R in Rot markiert eine Lücke im Rollenmodell Die Befunde beschreiben Konstruktionsmerkmale, keine Leistungsurteile.

Abb. 4.4: Tiefeninterviews und Rechts- und Governance-Rahmen GSÖ 2030

4.5 – DIE BAUSTEINE

Drei Entscheidungen schließen die Führungslücke

Ein Sicherheitsrat mit Weisungsrecht, ein ziviler Operationsplan und eine mandatierte Stelle für das Lagebild: Diese drei Entscheidungen lösen die gemeinsame Wirkung vom Zufall einzelner Personen. Für jeden Vorschlag liegt eine Beschreibung aus der Praxis vor. Eine zusätzliche Behörde braucht es dafür nicht.

Die drei Entscheidungen bedingen einander. Ohne gemeinsames Lagebild entscheidet der Sicherheitsrat ins Leere. Ohne zivilen Operationsplan bleibt offen, wer anschließend handelt. Ohne mandatierte Stelle bleibt der Plan Papier.

Der erste Baustein ist der Sicherheitsrat mit Weisungsrecht. Ansgar Rieks hat ihn als persönliche Sicht ausformuliert: einen hauptamtlichen Stabskern mit Leitung, entscheidungsbefugte Ressortvertreter, eine vorbereitende Arbeitsebene und darüber ein Gremium unterhalb von Kanzler und Ministern. Das Weisungsrecht entscheidet über die Wirksamkeit.



„Der Sicherheitsrat muss ins Mandat geschrieben bekommen, dass er eine Weisungskompetenz in die Häuser hat.“

Dr. Ansgar Rieks • Generalleutnant a.D. und Vorstandsmitglied, [AFCEA International](#)

Der zivile Operationsplan bildet den zweiten Baustein. Martin Zeidler vom BBK beschreibt die Größenordnung: Dem militärischen Werk von rund 1.500 Seiten fehlt ein ziviles Gegenstück. Ein ressortübergreifender Plan für Bund, Länder und Kommunen müsse eher eine Million Seiten umfassen. Leonard Wessendorff von Project Q bestätigt die laufenden Arbeiten, hat bislang jedoch keine konkreten Maßnahmen gesehen.

Das Mandat zur Lagebildverdichtung ist der dritte Baustein. Martin Zeidler nennt eine veränderte Mandatierung als entscheidenden Hebel. Sein Haus verfüge über Expertise, könne jedoch keine verbindlichen Standards setzen. Eine angepasste Befugnis würde einheitliche Prozesse unmittelbar ermöglichen.

Der Verkehrssektor zeigt, weshalb ein ziviler Operationsplan auf Prozesse zielen muss. Eine verantwortliche Person für Informationssicherheit bei der Bahn beschreibt die Leerstelle: Einzelne Leit- und Steuerungssysteme lassen sich umfassend absichern. Der Zugverkehr steht trotzdem, sobald Energie, Personal oder Vorleistungen ausfallen. Ein ziviler Plan muss deshalb betriebliche Abhängigkeiten und Prioritäten zusammenführen und darf sich nicht auf Anlagenlisten beschränken.

Strukturen entstehen anlassbezogen und werden nachträglich ausgestattet. Armin Fleischmann verweist auf das Gemeinsame Terrorismusabwehrzentrum und das Führungszentrum Nationale Luftverteidigung: mühsam erkämpft und jeweils auf einen Anlass zurückzuführen. Dr. Volker Pötzsch vom Kommando Cyber- und Informationsraum nennt das neue Zentrum zur Abwehr hybrider Bedrohungen organisatorisch richtig und rät zugleich zum Erwartungsmanagement.

Drei Lücken, drei Entscheidungen

DEFIZIT	WIRKUNGSVERLUST	BAUSTEIN	ZUSTÄNDIG
Sicherheitsrat ohne Weisungsrecht	Entscheidungen erreichen die Ressorts nicht.	► Mandat mit Durchgriff, hauptamtlicher Unterbau	Bundeskanzleramt
Kein ziviles Gegenstück zum Operationsplan	Nach der Entscheidung ist offen, wer was tut.	► Ressortübergreifender ziviler Operationsplan	Bundesministerium des Innern mit Ländern
Kein Mandat zur Lagebildverdichtung	Expertise ohne Standardsetzung erzeugt Empfehlungen.	► Strukturelle Änderung der Mandatierung	Bundesministerium des Innern für das BBK

Abb. 4.5: Tiefeninterviews GSÖ 2030

4.6 – DIE GESAMTVERTEIDIGUNG

Im Bündnisfall kehrt sich die Unterstützung um

Die zivil-militärische Schnittstelle wird in Deutschland als Amtshilfe gedacht. Die Bundeswehr kommt, wenn es zivil eng wird: bei der Flut, in der Pandemie, nach dem Sturm. Diese Erwartung hat sich über Jahrzehnte eingeschliffen und funktioniert im Frieden.

Im Verteidigungs- oder Bündnisfall braucht die Bundeswehr selbst Unterstützung. Marlis Cremer vom Deutschen Roten Kreuz beschreibt die zivile Seite dann als vierte Säule der Gesamtverteidigung: beim Host Nation Support für durchgeschleuste Truppen und bei der Unterstützung des Sanitätsdienstes, einer Kernaufgabe ihrer Organisation.



„Die Bundeswehr wird gerne als das bewaffnete THW gesehen. In der Ostflanke steht dieses bewaffnete THW aber nicht mehr zur Verfügung – dann ist die Bundeswehr Bittsteller gegenüber den zivilen Bereichen.“

Axel Lips • Associate Director Public, Defence & Security, Sopra Steria

800.000

Kräfte werden im Bündnisfall binnen eines halben Jahres durch Deutschland transportiert.

Operationsplan Deutschland

Wolfgang Gäbelein von der Deutschen Gesellschaft für Wehrtechnik beschreibt die gleichzeitigen Anforderungen. Vier Ströme teilen sich Korridore und konkurrieren um knappe Ressourcen: die deutschen Streitkräfte mit eigenem Bedarf, die Partner auf dem Weg in die Einsatzgebiete, ein gegenläufiger Strom von Flüchtenden und ein Gesundheitswesen, das Verwundete und Bevölkerung versorgen muss. Wer diese vier Ströme priorisiert, ist nicht geregelt.

Auf der zivilen Seite fällt zugleich weg, worauf man sich eingerichtet hat. Leif Erik Sander von der Charité benennt es: Formen der Unterstützung durch die Bundeswehr, an die sich Landräte und

Kommunen im Frieden gewöhnt haben und die bislang vieles abgepuffert haben, stehen im Spannungsfall nicht mehr zur Verfügung. Die Konsequenzen sind im fragmentierten zivilen System kaum durchdacht. Albrecht von Croÿ vom Malteser Hilfsdienst zieht daraus eine Warnung: Mit Blick auf den Operationsplan dürfe man mit der Bundeswehr für solche Aufgaben künftig nicht mehr rechnen, weil sie das nicht mehr könne und nicht mehr wolle. Den Betrieb von Pflegeheimen in einer Pandemie aufrechtzuerhalten, gehöre nicht zum militärischen Auftrag.

Im hybriden oder im Spannungsfall fällt damit ein zweites Sicherungsnetz aus. Bei einer flächigen Lage steht auch die gegenseitige Unterstützung aus anderen Teilen der Republik nur eingeschränkt zur Verfügung.

Die Schnittstelle scheitert zuerst an der Sprache, erst danach an der Technik. Benedikt Meng von infodas beschreibt die Folge fehlender gemeinsamer Führungsinformationssysteme: Ein Polizeihauptkommissar muss im Gefechtsstand einer Heimatschutzkompanie übersetzen, was er sieht. Übungen mit Partnern hätten genau das zutage gefördert: Der Zugriff auf gemeinsame Systeme und kompatible verschlüsselte Funkgeräte fehlt. Eine organisatorisch verankerte Verbindung bietet das Landeskommmando Bayern. Thomas Hambach ist dort erster Ansprechpartner für die Staatsregierung für Bundeswehrfragen und arbeitet zugleich mit den Bezirksregierungen. Die Landeskommandos verbinden damit Länder und Kommunen dezentral mit der militärischen Lageführung.

Dass diese Schnittstelle praktisch geübt wird, zeigt CIMIC Quadriga 2026. Vom 14. bis 26. Juni übten in Niedersachsen Soldatinnen und Soldaten aus 28 Nationen mit Polizei, Feuerwehr, Hilfsorganisationen, Kliniken, Verwaltungen und Unternehmen. Mehr als 150 Lageeinweisungen bildeten unter anderem die Drehscheibe Deutschland im Bündnisfall ab.

Der militärische Plan braucht ein ziviles Gegenstück

Die zivile Seite kann sich selbst verbinden. Der Kreis Neuwied grenzt unmittelbar an Nordrhein-Westfalen und pflegt neben den rheinland-pfälzischen Nachbarkreisen kontinuierlichen Austausch zum Rhein-Sieg-Kreis: wechselseitige Fortbildungen, ein operatives Netzwerk, gegenseitige Unterstützung bei großen Schadenslagen. Volker Lemgen von der Kreisverwaltung nennt das strukturelle Argument dafür schlicht: Brände halten nicht an der Landesgrenze, also kann die Praxis das auch nicht. Zur Bundeswehr besteht dieselbe Architektur, sie wurde bislang nur nicht in Anspruch genommen: keine operative Anforderung, eine besuchte Übung. Das Technische Hilfswerk dagegen wird regelmäßig gerufen. Was zivil geübt ist, funktioniert. Was militärisch angelegt ist, wartet auf den ersten Fall.



„Es fehlt mit Sicherheit der zivile Teil – ich würde es umdrehen: bisher ist nur der militärische Teil existent. Für mich ist der zivile Teil der viel größere.“

Gerald Funke • Generalleutnant, Befehlshaber Unterstützungskommando, Bundeswehr

Auf Bündnisebene wächst die Führungsfrage um eine weitere Stufe. Ansgar Rieks von AFCEA International verweist auf die bestehende Kommandostruktur mit Gefechtsstand für alliierte Luftstreitkräfte und Ausweichstandorten in Europa. In der Debatte über einen Abzug amerikanischer Kräfte komme es darauf an, diese Struktur zu erhalten. Unsicherheit sieht er auch in Europa: Manche Partner wollten eine neue europäische Ordnung, unterstützten die vorhandene Kommandostruktur jedoch unzureichend.

BÜNDNISFALL

Im Bündnisfall kehren sich die Rollen um



VERTEIDIGUNGS- ODER BÜNDNISFALL

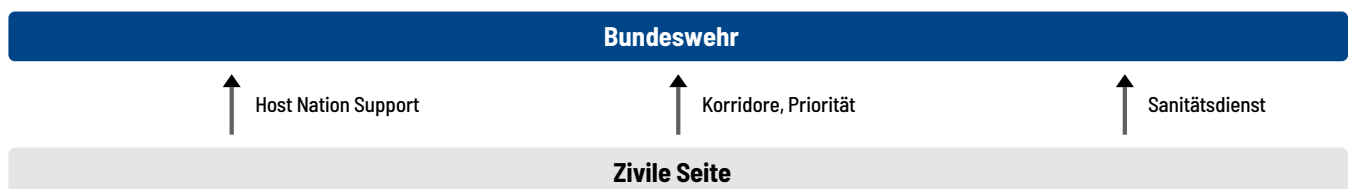


Abb. 4.6: Tiefeninterviews GSÖ 2030

4.7 – DIE VERSORGUNG

Wer im Ernstfall Vorrang hat, ist nicht geregelt

Das KRITIS-Dachgesetz erfasst registrierte Betreiber mit Meldepflichten und Mindeststandards – zum 30. Juni 2026 waren es 1.231 Betreiber mit 2.180 Anlagen. Mit der Umsetzung der NIS-2-Richtlinie wächst dieser Kreis auf schätzungsweise 33.000 Unternehmen. Das Versorgungsrisiko reicht auch dann weiter: Zahlreiche Unternehmen sind für den Ernstfall unverzichtbar, ohne erfasst und priorisiert zu sein.

Tankstellen sind keine kritische Infrastruktur, aber ohne Treibstoff fährt kein Einsatzfahrzeug, kein Notstromaggregat läuft nach, keine Lieferkette bewegt sich.



„Im Großraum Bonn gibt es eine einzige Tankstelle mit Notstromversorgung. Eine im ganzen Großraum.“

Thomas Tschersich • CSO, Deutsche Telekom

Armin Fleischmann verortet die Ursache in der Friedensdividende: Vieles, was früher staatlich war, wurde ausgelagert und dezentralisiert – IT, Betrieb, Versorgung. Die Leistung blieb, die staatliche Verfügungsgewalt darüber nicht.

Entscheidend ist die Priorisierung im Ernstfall. Der Staat kann heute nicht sagen, welches Unternehmen Strom behält. Hanno Friedrich von der Kühne Logistics University zeigt die Folge an den Abschaltplänen im Energiesystem: Sie priorisieren keine einzelnen Unternehmen. Die Netztopologie entscheidet, wer vom Strom getrennt wird. Eine Brotfabrik, ein Rechenzentrum und ein Möbelhaus am selben Strang werden gleich behandelt.

Der Blick auf die Verkehrsinfrastruktur zeigt die nächste Blindstelle.

Peter Holm vom Bundesverband Güterkraftverkehr verweist auf rund 4.500 marode Brücken. Für den Operationsplan wird daraus eine Sicherheitsfrage: Die Bewegung von bis zu 800.000 Kräften durch Deutschland hängt von Bauwerken ab, die in keinem Sicherheitsregister stehen. Hinzu kommt der fehlende Zugriff auf einen Teil der Lastkraftwagen, die ausländischen Unternehmen gehören.

Vorsorge scheitert dabei selten am Recht, meist an der Aufmerksamkeit.

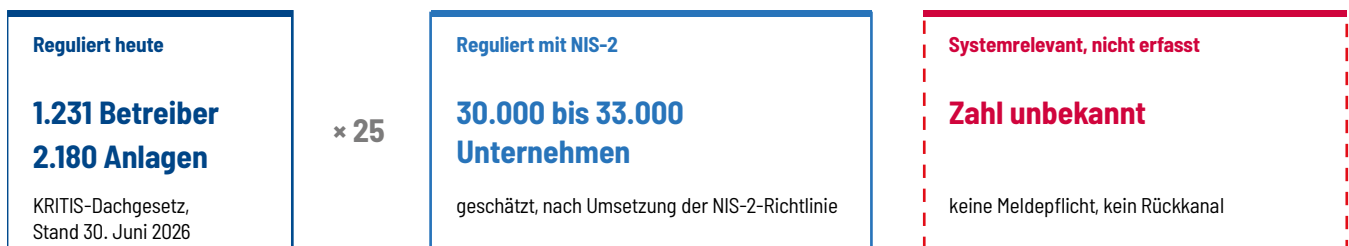
Peter Holm verweist auf die Erhebungen des Business Continuity Institute: Die meisten Unternehmen werden erst dann aktiv, wenn bereits etwas passiert ist. Einer Vorsorgevereinbarung mit der Industrie steht dabei keine gesetzliche Bedingung entgegen.

Christian Growitsch vom HIICCE beschreibt die Folgen für die Produktion im Ernstfall: Relevante Rüstungsgüter entstehen aktuell im Manufakturbetrieb, während Deutschland Fahrzeuge hocheffizient in Serie fertigt. Seine Forderung: moderne Fertigungsverfahren auch in der Verteidigungsindustrie einsetzen.

Der regulierte Bereich verschiebt sich, das reale Risiko nicht.

KRITIS

Der regulierte Bereich verschiebt sich, das reale Risiko nicht



Energie · Wasser · Telekommunikation · Verkehr · Gesundheit

Beispiele

- Tankstellen mit Notstrom
- rund 4.500 marode Brücken
- Beatmungs-Wohngemeinschaften

Abb. 4.7: BSI-Registrierung und Tiefeninterviews GSÖ 2030

Souveränität heißt priorisieren können

Souveränität ist die vorab geregelte Fähigkeit, im Krisenfall priorisiert beziehen zu können. Vollständige Eigenproduktion ist dafür nicht erforderlich. Die Lieferketten reichen tiefer, als die Regulierung blickt. Frank Scholz von MilDef zeigt das an der eigenen Fertigung: Schlüsselkomponenten wie Speicher und Bildschirmpanels kommen ausschließlich aus Taiwan. Peter Kuhne von der IHK Bonn/Rhein-Sieg nennt eine Abhängigkeit auf der nächsten Stufe: Der Sprengstoff für Munition stammt weitgehend aus China, hochfeste Stähle kommen aus Indien. Diese Risiken liegen bei den Zulieferern und deren Vorlieferanten. Hanno Friedrich benennt die Datenlücke dahinter: Niemand kennt die sektorübergreifenden Verflechtungen zwischen den Unternehmen vollständig.



„Der Staat muss die Lebensmittelwirtschaft befähigen zu arbeiten – das ist seine Rolle, nicht selbst Lebensmittel herzustellen.“

Prof. Dr. Hanno Friedrich • Associate Professor for Transport, [Kühne Logistics University](#)

Befähigen setzt voraus, dass beide Seiten wissen, worum es geht.

Friedrich zeigt an der Erfahrung mit NIS-2, dass das nicht gegeben ist: Obwohl Bußgelder drohten, habe sich nur etwa die Hälfte der erwarteten Unternehmen registriert. In Logistik und Lebensmittelwirtschaft dürften es kaum zehn Prozent sein.

Große kritische Betreiber fragen längst nach den relevanten Szenarien und gelten aus Sicht der Landeskommmandos als operativ vorbereitet. Thomas Tschersich bestätigt das für Energieversorger und Kernnetze. Der Engpass liegt eine Ebene tiefer. Die Arbeit von Defence.NRW zeigt, dass sich viele mittelständische Unternehmen trotz täglicher Berichte für unbetroffen halten. Sven Hallbauer von der EWERK Group kennt Fälle, in denen bereits eine Firewall für zehntausend Euro fehlt.

Ein Beispiel aus der Versorgung zeigt die Reichweite dieser

Definitionsgrenze. Michael Kreinest von der BG Klinik Ludwigshafen verweist auf Wohngemeinschaften beatmungspflichtiger Menschen ohne Notstromversorgung, nur der Geräteakku trägt wenige Stunden. Sie zählen nicht zur kritischen Infrastruktur, unterliegen keiner Meldepflicht, und sein Team musste ihre Standorte selbst recherchieren. Der regulierte Bereich deckt das reale Risiko daher nur teilweise ab. Benötigt wird eine Stelle, die im Ernstfall priorisiert: welches Unternehmen Strom behält, welche Brücke zuerst ertüchtigt wird und welche Abhängigkeit vertraglich abzusichern ist. Dieses Mandat fehlt bereits bei der gesamtstaatlichen Führung. Seine Wirkung reicht bis in die Lieferkette.

4.8 – DAS MANDAT

Entscheidungen für eine handlungsfähige Sicherheitsarchitektur

Bis 2030 stehen sieben institutionelle Entscheidungen an. Sie folgen aus den Befunden dieses Kapitels und verlangen weder eine neue Behörde noch eine Änderung des Grundgesetzes. Kapitel 7 übersetzt sie in Maßnahmen mit Träger, Frist und Nachweis.

Ein Mandat mit Weisungsrecht. Der Nationale Sicherheitsrat braucht die Befugnis, in die Ressorts hinein zu entscheiden, und einen hauptamtlichen Unterbau, der zwischen den Sitzungen arbeitet. → **7.3**

Ein ziviler Operationsplan. Das Gegenstück zum militärischen Plan, das Bund, Länder und Kommunen einschließt und benennt, wer nach einer Entscheidung was tut. → **7.3** und **7.6**

Eine mandatierte Stelle für das Lagebild. Fachliche Expertise ohne die Befugnis, Standards zu setzen, erzeugt Empfehlungen, keine Wirkung. → **7.2**

Ein Rückkanal an die Betreiber. Wer meldepflichtig ist, muss Lagebildzugang, Frühwarnung und priorisierte Ressourcen zurückbekommen, sonst bleibt die Meldung eine Pflichtübung. → **7.2**

Eine definierte Übergangsschwelle. Wann die Verantwortung von der kommunalen auf die Landes- und weiter auf die Bundesebene wechselt, steht heute in keinem Gesetz. → **7.3**

Eine Priorisierungsregel für die Wirtschaft. Abschaltpläne, Korridore und Vorsorgevereinbarungen brauchen eine Stelle, die im Ernstfall entscheidet, wer zuerst versorgt wird. → **7.4**

Ein geübtes zivil-militärisches Verfahren. Gemeinsame Lagebilder und abgestimmte Prioritäten müssen vor dem Ernstfall durchlaufen worden sein, nicht in ihm. → **7.6**

In Neuwied vergingen vierzig Stunden ohne zentrale Einsatzleitung, im Ahrtal erreichten Meldungen ihre Adressaten, ohne dass ein Auftrag folgte. Gebraucht wird eine schnell verfügbare Reserve, im BBK verankert, die diese Anlaufphase überbrückt, bis die reguläre Struktur greift. → **7.6**

Vier Adressaten, nicht mehr

- **Bundeskanzleramt** – Mandat und Weisungsrecht. Ohne diesen Schritt bleibt alles Weitere Vorbereitung.
- **Bundesministerium des Innern (BMI)** – ziviler Operationsplan, Mandatierung für das Lagebild, Rückkanal an die Betreiber.
- **Länder** – die Übergangsschwelle, weil sie ohne ihre Zustimmung nicht definierbar ist.
- **Betreiber** – die Abhängigkeiten unterhalb der ersten Ebene, die nur sie kennen.

Die Bundeswehr ist in dieser Liste Beteiligte, nicht Adressatin. Ihre Seite der Schnittstelle ist geregelt, die zivile ist es nicht. Zwei Punkte haben ein offenes Fenster. Die Überprüfung der Vorsorge- und Sicherstellungsgesetze läuft seit dem Beschluss vom 8. Juni 2026 – wer den Krisendatenaustausch und die Betreiberpflichten geregelt sehen will, muss sie in dieses Verfahren einspeisen, nicht danach. Und der Steuerungsstab für die zivile Verteidigung entsteht gerade, ob er Durchgriff bekommt, entscheidet sich bei seiner Ausgestaltung, nicht später.

Die erste Entscheidung trägt alle weiteren. Ohne Mandat produziert jede technische Kopplung Anschlussfähigkeit ohne Anschluss. Das digitale Rückgrat ist daher keine IT-Frage, sondern eine Governance-Frage.

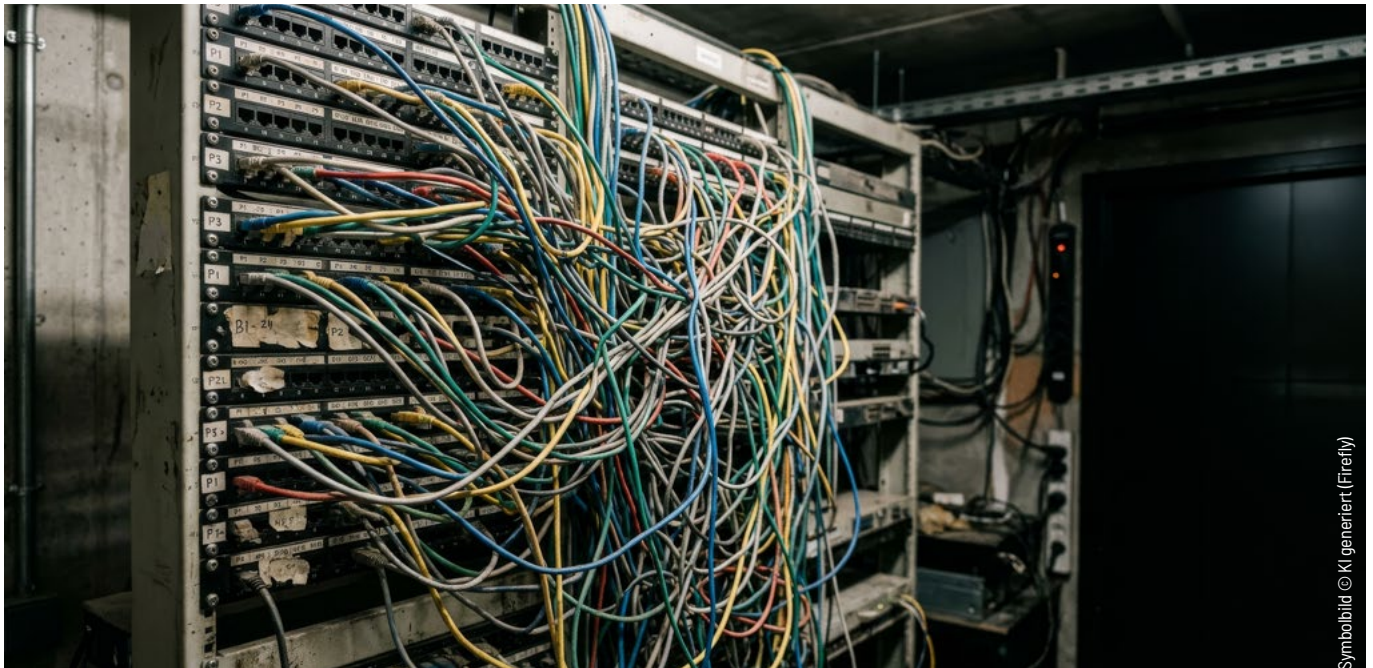
05

Das digitale Rückgrat

Kopplungsfähigkeit statt einer Plattform

5.0 – DIE AUSGANGSLAGE

Die Daten sind da, die Verbindung fehlt



Symbolbild © KI generiert (Firefly)

Daten liegen in vielen Systemen bereit. Wirkung entsteht, sobald sie über Organisations- und Sicherheitsgrenzen hinweg rechtzeitig zusammenfinden. Kapitel 5 folgt den acht Technologie-Domänen und den Übergängen, an denen diese Kopplung heute stockt.

Kopplungsfähigkeit beginnt bei offenen Übergängen. Standards existieren vielfach. Schwierig sind Zugang, Einstufung, Rollenrechte und die Vielzahl einzelner Punkt-zu-Punkt-Verbindungen. Das digitale Rückgrat ist auf eigenständige Systeme mit verbindlichen Schnittstellen angewiesen. → [5.1](#)

Fünf Aufgaben bilden den Funktionsraum: Lage erfassen und teilen, Entscheidungen vorbereiten, Handeln koordinieren, Wirkung unterstützen sowie Betrieb sichern und wiederherstellen. Dazwischen liegen vier Übergänge, an denen Informationen, Rechte oder Rückkopplung abbrechen. Aus dem abstrakten Verbindungsproblem wird damit ein nachvollziehbarer Ablauf. → [5.2](#)

Acht Technologie-Domänen tragen diesen Ablauf. Für drei davon weist der erfasste Bestand keine Lösung aus: Logistik- und Ressourcensteuerung, Resilienz und Wiederanlauf sowie Governance und Zugriff. Vorhandenes Angebot und echte Angebotslücke lassen sich damit trennen. → [5.3](#)

Der meistgenannte digitale Mangel ist das gemeinsame Lagebild: 18 von 47 Antwortenden nennen es als unverzichtbare Grundlage, 16 von 47 als kritischsten Engpass. Zugleich fehlt für die Kopplungsschicht ein eindeutiger Käufer. Technische Lücke und fehlende Nachfrage führen auf denselben institutionellen Punkt zurück. → [5.4](#)

Die Ukraine liefert einen belastbaren Gegenbeleg zur Vorstellung, verteilte Systeme ließen sich unter Druck kaum verbinden. Delta koppelt unterschiedliche Quellen und Zuständigkeiten, während die Verantwortung dezentral bleibt. Übertragbar ist die Bauweise einer Kopplungsschicht, nicht das System. → [5.5](#)

Aus dem Vergleich ergibt sich eine Reihenfolge für Deutschland: Datensprache und Rechte klären, Schnittstellen verbindlich machen, Rückfallebenen sichern und Zykluszeit messen. Erst danach kann Beschaffung skalieren. Aus der technischen Diagnose wird damit ein Transformationspfad. → [5.6](#)

5.1 – DIE KOPPLUNGSFÄHIGKEIT

Verbunden, nicht verschmolzen

Gemeint ist keine enge Integration. Systeme bleiben eigenständig und werden nur so weit verbunden, wie die gemeinsame Wirkung es verlangt. Denn eng gekoppelte Systeme reißen im Ausfall alles mit. Kopplungsfähigkeit umfasst mehr als Vernetzung. Sie verlangt neben der technischen Verbindung geklärtes Recht, abgestufte Rollen und eine gemeinsame Datensprache. Der Markt liefert diese Verbindung nicht, eine Hierarchie erzwingt sie zu teuer. Erst als Ökosystem entsteht sie: verbindlich im Auftrag, eigenständig im Betrieb.

Drei Antworten bestimmen die deutsche Debatte: eine zentrale Plattform, die Behördencloud und eine vollständig vorab entworfene Architektur. Jede greift zu kurz, weil sie den Blick auf die Vermeidung des Ausfalls richtet. Entscheidend ist die Fähigkeit, einen Treffer zu verkraften und schnell weiterzuarbeiten.

„Wie in jedem Boxkampf werden Sie auch einen Treffer abbekommen. Die Frage ist, ob Sie trainiert sind, ihn wegzustecken und schnell wieder handlungsfähig zu sein.“

Dr. Volker Pötzsch • Generalmajor Kommando Cyber und Informationsraum, Bundeswehr

Eine zentrale Plattform verspricht Ordnung, schafft jedoch einen gemeinsamen Ausfallpunkt. Ihr Betreiber müsste zudem für Akteure handeln, die ihm nicht unterstellt sind. Widerstandsfähigkeit entsteht dagegen durch verteilte Standorte und belastbare Übergänge.

Die Behördencloud beantwortet die Betriebsfrage. Delos Cloud läuft, Google Cloud entsteht bei der BWI, secunet baut eine Cloud für Verschlusssachen auf. Ungeklärt bleiben die Verbindungen zwischen diesen Angeboten.

Die dritte Antwort verlangt eine vollständige Definition vor dem Bau. Das kostet Zeit und friert den Entwurf früh ein. Anbieter fordern daher eine Architektur, die mit einer tragfähigen Grundstruktur beginnt und fortlaufend wächst.

Drei Eigenschaften machen Kopplungsfähigkeit im Betrieb aus: Verlegefähigkeit, Redundanz und Interoperabilität. Bernd Reitmeier von Bechtle hört sie bei Kunden immer wieder. Sie entstehen aus Bauweise, Regeln und Übung – kein Beschaffungsvertrag liefert sie.

Interoperabilität hat vier Ebenen: Recht, Rollen, Datensprache und Technik. Die Technik ist am weitesten entwickelt, die größeren Hürden liegen darüber.

Der Bund ist sein eigener größter Nutzer und Geldgeber. Sven Hallbauer von der EWERK Group zieht daraus einen einfachen Schluss: „Die Mittel kommen von mir, der Nutzer bin ich selbst – warum mache ich es dann nicht gleich richtig, mit offenen Standards?“ Statt jahrelang Kompromisse zu moderieren, könnte der Bund auf Basis offener Standards eine Lösung bauen, sie offen bereitstellen und vorangehen. Ist sie gut genug, folgen die Länder von selbst.

Im Verteidigungsbereich ist Open Source längst Praxis, nicht Programm. Die BWI betreibt einen Matrix-basierten Messenger im Wirkbetrieb, Ende-zu-Ende-verschlüsselt und auf eigener Infrastruktur förderierbar. Sie baut zwei Cloud-Standbeine auf Open-Source-Basis auf, eines davon feldtauglich: ein Rechenzentrum in Kofferformat. Für die private Cloud der Bundeswehr verfolgt sie einen Multi-Cloud-Ansatz aus mehreren, gegeneinander absicherbaren Bausteinen.

INTEROPERABILITÄT

Drei Ebenen brechen, eine trägt

EBENE

Recht

Was darf geteilt werden?

Rollen

Wer darf was sehen?

Datensprache

Was bedeuten die Daten?

Technik

Wie verbinden sich Systeme?

Abb.5.1 Tiefeninterviews GSÖ 2030

WAS HEUTE BRICHT

Einstufungen verhindern das Teilen von Lagebildern

Rollen und Rechte sind nicht abgestuft geregelt

Wann gilt ein Bett als frei? Nicht einheitlich definiert

Standards existieren – SINA, MCX, BroadWay

5.2 – DAS ZUSAMMENSPIEL

Die Systeme stehen, die Verbindung dazwischen nicht

Die technische Grundlage muss fünf Aufgaben tragen: Lage erfassen und teilen, Entscheidungen vorbereiten, Handeln koordinieren, Wirkung unterstützen sowie den Betrieb sichern und wiederherstellen. Kapitel 3 beschreibt die dafür nötigen Fähigkeiten, hier geht es um ihre Verbindung.

Für jede Aufgabe bestehen Systeme und Zuständigkeiten. Die fünf Aufgaben verbinden vier Übergänge — und jeder bricht auf seine Weise.

„Es ist nicht alles ein technologisches Problem — es ist ein Problem der Architektur und der Governance: Wer darf welche Daten austauschen?“

Hans-Martin Zimmermann • Head of Engineering Defence Digital, Airbus Defence and Space

Die erste Bruchstelle liegt zwischen Erfassen und Entscheiden. Daten müssen zu belastbaren Informationen verdichtet werden. Wolfgang Gäbelein von der Deutschen Gesellschaft für Wehrtechnik nennt das ebenengerechte Verdichtung. Heute übernehmen häufig Menschen diese Arbeit, indem sie Angaben aus mehreren Systemen manuell übertragen und aufbereiten.

Die zweite Bruchstelle betrifft die Rechte zwischen Entscheiden und Koordinieren. Sven Weizenegger vom Cyber Innovation Hub der Bundeswehr fordert ein System, das Daten aus verschiedenen Sicherheitsbereichen zusammenführt und die Sicht je Rolle begrenzt. Feuerwehr und Bundeswehr benötigen unterschiedliche Ausschnitte. Technisch ist das möglich, die Architektur bleibt offen. Die Tabelle auf dieser Seite führt die vier Übergänge einzeln auf: was an jedem gebraucht wird und wo das Marktangebot endet.

Die dritte Bruchstelle trennt Koordination und Wirkung. Martha Klare von der Universität der Bundeswehr München beschreibt die Distanz zwischen Datentechnik und den Anlagen, die Strom, Gas oder Wasser steuern. In vielen Unternehmen der kritischen Infrastruktur bleiben beide Welten getrennt. Ein gemeinsamer Blick auf Anomalien würde Eingriffe ermöglichen, bevor sich eine Störung fortsetzt.

Die vierte Bruchstelle liegt zwischen Einsatz und Wiederanlauf. Erkenntnisse aus einer Lage fließen selten geordnet zurück. Martin Zeidler vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe unterscheidet Pflicht und Kür: Grunddaten sichern die Lagebewältigung, ihre Verknüpfung ermöglicht Prognose und Nachbereitung. Der zweite Schritt unterbleibt häufig.

Alle vier Übergänge leiden unter demselben Maßstab. Der behördliche Führungsvorgang prüft die Vollständigkeit. In schnell wechselnden Lagen zählt zusätzlich die Zykluszeit vom Beobachten über Einordnen und Entscheiden bis zum Handeln. Ein vollständiger Prozess kann zu spät kommen.

Standards, offene Software und förderierbare Komponenten existieren. Der Bruch liegt beim Zugang, bei der verbindlichen Forderung in der Beschaffung und bei der organisationsübergreifenden Nutzung.

FUNKTIONSRaum

Vier Übergänge, vier Brüche



DIE VIER ÜBERGÄNGE

- 1 Verdichtung**
Aus vielen Meldungen wird ein entscheidungsreifes Bild — oder keines.
- 2 Rechtefrage**
Wer darf im Ernstfall sehen und entscheiden?
- 3 Trennung von Informations- und Betriebstechnik**
Zwischen Lagebild und Wirksystem liegt eine Grenze.
- 4 Übergang zum Wiederanlauf**
Kein Marktangebot deckt diesen Übergang ab.

Abb. 5.2: Tiefeninterviews und Lösungs-Datenbank GSÖ 2030

Verbindung wird gefordert, nicht angeboten

Zwischen dem, was gebraucht wird, und dem, was der Markt liefert, klafft nirgends eine so große Lücke wie bei der Datenintegration. Die Befragung beziffert sie.

25 zu 5

Bedarfsnennungen zu Lösungsangeboten bei Datenintegration und Interoperabilität. Das ist die größte Diskrepanz in der Befragung.

GSÖ-Befragung unter Technologieanbietern und Anwendern, Lösungs-Datenbank GSÖ 2030

Was gefordert wird, lässt sich beschreiben. Wolfgang Gäbelein zeigt es an einer Staudammsprengung: Menschen vor Ort signalisieren, dass Einsatzkräfte gebraucht werden, und das fließt ins Gesamtlagebild zurück, egal über welchen Kanal. Dort genügt die Information, dass der Grenzwert überschritten ist. Den Wasserstand auf den Zentimeter genau braucht niemand.

Dass es geht, zeigt die Ukraine. Beide Fähigkeiten entstanden dort unter Beschuss: Die Anwendung eVorog speist Beobachtungen der Bevölkerung in das Lagebild ein, Starlink hält die Verbindung aufrecht, sobald die eigene Infrastruktur ausfällt.

Auch in Deutschland gibt es ein Beispiel. Das Kommando Cyber- und Informationsraum bündelt vier Säulen aus einer Hand – Cyber, IT, Informationsraum samt elektromagnetischem Spektrum und Geo-informationswesen. Der Mehrwert liege darin, dass Themen, die früher verteilt waren, abgestimmt auf Lagen reagieren.

Die Aufgabe selbst ist überschaubar. Hanno Friedrich von der Kühne Logistics University führt sie auf vier Grundfunktionen zurück: koordinieren, kommunizieren, Meldungen empfangen und reaktionsfähig bleiben. Praktisch brauche es zweierlei – eine Landkarte des Lebensmittelökosystems, die zeigt, wer wo sitzt und was tut, und ein Risiko- und Kommunikationssystem, über das Unternehmen Probleme melden und die zuständigen Stellen die aufbereitete Information erhalten. Acht Technologie-Domänen tragen diese Aufgaben – von Lagebild und Sensorik bis Governance und Zugriff.

Die Lücken im Angebot sind klar erkennbar. Abbildung 5.4 zeigt zwei Arten: Erstens ist bei der Datenintegration die Nachfrage hoch und das Angebot dünn. Zweitens ist bei Ressourcensteuerung, Wiederanlauf und Zugriff beides niedrig. Die eine Lücke schließt eine Beschaffungsentscheidung, die andere erst eine Bedarfsdefinition.

Der folgende Abschnitt prüft, was der Markt in jeder davon anbietet.

NACHFRAGE

Am häufigsten genannt, am schwächsten bedient

TECHNOLOGIE-DOMÄNE

		Lage erfassen und teilen	Entscheidungen vorbereiten	Handeln koordinieren	Wirkung unterstützen	Betrieb sichern und wiederherstellen	BEDARF	LÖSUNGEN
D1	Lagebild & Sensorik	●	○				21	14
D2	Datenintegration	●		○			25	5
D3	Kommunikation			●	○		28	24
D4	Führung & Entscheidung		●	○			19	12
D5	Cyber- & Informationssicherheit	○	○	○	○	●	15	4
D6	Logistik- & Ressourcensteuerung				●	○	5	0
D7	Resilienz & Wiederanlauf					●	4	0
D8	Governance & Zugriff	○	●	○			4	0

● trägt die Funktion

○ trägt mit

Marktbefund je Domäne aus der GSÖ-Befragung, N = 72

Zuordnung abgeleitet aus den Fähigkeitsbezügen F0 bis F7 je Technologie-Domäne (Annex 6).
Rote Markierung: keine Lösung im erfassten Marktangebot.

Abb. 5.3 GSÖ-Befragung und Lösungs-Datenbank GSÖ 2030

5.3 – DIE TECHNOLOGIE-DOMÄNEN

Wo das Marktangebot trägt

Kritisch ist jene Informationstechnik, deren Ausfall die Wirkung über Sektorgrenzen hinweg mindert. Acht internationale Beispiele zeigen, was in den einzelnen Domänen möglich ist. Nur eines stammt aus Deutschland.

Die Erfassung ist technisch weit entwickelt. Nach dem Erdbeben in der Türkei und in Syrien im Februar 2023 erzeugte xView2 binnen Stunden aus Satellitenbildern ein Schadenslagebild von mehr als 160.000 eingestürzten Gebäuden. Das quelloffene Projekt entstand im Umfeld des Pentagon.

Bei der Verbindung liegt Deutschland zurück. Estlands X-Road koppelt 99 Prozent der staatlichen Datenbankdienste, zivile wie militärische, ohne eine zentrale Datenhaltung zu schaffen.

Europa hat grenzüberschreitende Kommunikation erprobt: Im Projekt BroadWay testeten elf Länder ein gemeinsames Behördenbreitband. Japan zeigt die nächste Stufe. Der Rechner Fugaku simuliert mehr als 30.000 Szenarien gleichzeitig und unterstützt, verbunden mit dem nationalen Warnsystem, die Evakuierungsplanung bis auf Bezirksebene.

Für die Informationssicherheit dokumentieren die Unterlagen kein Werkzeug, dafür einen Angriff. Meliorator erzeugte automatisiert Tausende gefälschte Profile, die in Deutschland, der Ukraine und den Vereinigten Staaten aktiv waren. Vier westliche Nachrichtendienste bestätigten den Einsatz im Juli 2024.

Für die Ressourcensteuerung liefert ein Portal der Federal Emergency Management Agency (FEMA) das Beispiel: Es gleicht kommunale Bedarfe mit verfügbaren Hilfsressourcen ab. Ein durch künstliche Intelligenz gestütztes Schadenslagebild unterstützt die Priorisierung. Deutschland verfügt über keine vergleichbare Instanz.

Für Wiederanlauf und Zugriff stehen zwei weitere Beispiele. Nach einem Hurrikan ersetzten stratosphärische Ballons in Puerto Rico die ausgefallene bodengebundene Telekommunikation. Brandenburg schuf nach den Waldbränden einen gemeinsamen Informationsraum für Sicherheitsbehörden mit rollenbasiertem Zugriff.

Brandenburg liefert das einzige deutsche Beispiel dieser Reihe. Drei Technologie-Domänen bleiben dagegen unbesetzt: Ressourcensteuerung, Wiederanlauf und Zugriffsrechte. Damit fehlen Angebote ausgerechnet bei der Verteilung knapper Mittel, der Fortführung des Betriebs und dem geregelten Datenzugriff.

Wo das Angebot trägt

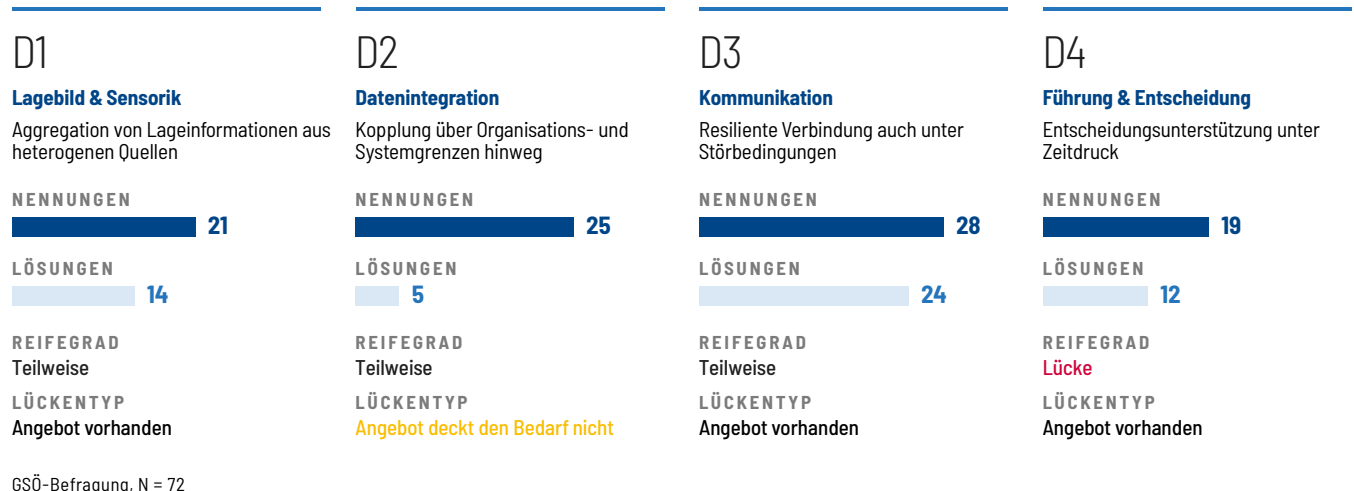


Abb. 5.4: GSÖ-Befragung und Lösungs-Datenbank GSÖ 2030

Drei Technologie-Domänen sind unbesetzt

Nicht jede Lücke lässt sich auf dieselbe Weise schließen. Was in Deutschland fehlt, hat drei verschiedene Ursachen – und jede verlangt eine andere Antwort.

Erstens fehlt mitunter die Verbindung. Vorhandene Systeme tauschen keine Daten aus. Bei der Datenintegration können verbindliche Schnittstellen dieses Defizit vergleichsweise schnell beheben.

Zweitens kann die Fähigkeit selbst fehlen, etwa bei souveräner Aufklärung, redundanter Satellitenkommunikation oder einer eigenen Technologiebasis. Dann ist Aufbauarbeit erforderlich.

Drittens kann das Regelwerk den Zugriff verhindern. Eine starre physische Trennung kappt Verbindungen, die im Ernstfall gebraucht werden. Vorschriften erzeugen operative Blindheit, sobald Streitkräfte verfügbare Fähigkeiten künstlicher Intelligenz nicht nutzen dürfen. Die Korrektur muss dann im Regelwerk ansetzen.

Der dritte Fall verlangt eine Sicherheitsabwägung. Israel erlebte 2020 die praktische Bedeutung der Trennung von Informations- und Betriebstechnik, als iranische Angreifer die Steuerung der Wasserinfrastruktur ins Visier nahmen. Die USA änderten nach dem Solar-Winds-Angriff ihr Prüfprinzip: Vertrauen gilt seither nur unter fortlaufender Kontrolle und schneller Reaktion.



„Ich plädiere nicht für totale Autarkie – aber Souveränität müsste sich als durchgehende Dimension durch alles hindurchziehen.“

Benedikt Meng • Leiter Business Development & Strategie, [infodas](#)

Wolfgang Koch vom Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie führt das aus: National sei nicht alles erreichbar, europäisch jedoch mehr. Spezialchips für militärische Anwendungen ließen sich in Deutschland fertigen. Bei generativer künstlicher Intelligenz gehe es um spezialisierte Modelle, nicht um das nächste große Sprachmodell. Über alle acht Domänen zeigt sich ein Muster: Verkaufbare Einzelprodukte sind vorhanden, verbindende Leistungen bleiben dünn.

Wo das Angebot fehlt

D5

Cyber- & Informationssicherheit

Schutz- und Vertrauensarchitektur des Rückgrats

NENNUNGEN

15

LÖSUNGEN

4

REIFEGRAD

Teilweise

LÜCKENTYP

Angebot deckt den Bedarf nicht

GSÖ-Befragung, N = 72

D6

Logistik- & Ressourcensteuerung

Steuerung knapper Ressourcen über Sektoren hinweg

NENNUNGEN

5

LÖSUNGEN

keine

REIFEGRAD

Lücke

LÜCKENTYP

Bedarf ohne Angebot

D7

Resilienz & Wiederanlauf

Absicherung, Redundanz und Wiederherstellung

NENNUNGEN

4

LÖSUNGEN

keine

REIFEGRAD

Teilweise

LÜCKENTYP

Bedarf ohne Angebot

D8

Governance & Zugriff

Identität, Zugriffsrechte, Audit-Trail

NENNUNGEN

4

LÖSUNGEN

keine

REIFEGRAD

Teilweise

LÜCKENTYP

Bedarf ohne Angebot

Abb. 5.5: GSÖ-Befragung und Lösungs-Datenbank GSÖ 2030

5.4 – DIE NACHFRAGE

Der Kopplungsschicht fehlt der Käufer

Sensoren, Funktechnik und einzelne Führungswerkzeuge lassen sich kaufen. Für die Kopplungsschicht fehlt die Stelle, die sie bestellt.

Die Lösungs-Datenbank erfasst 172 Einträge. 19 davon beziehen sich auf das Zusammenführen von Akteuren und Daten. Für keine ist ein Praxiseinsatz belegt. Es ist derselbe Befund, den Kapitel 3 für die Orchestrierung ausweist – nur auf der technischen Seite. Aussagen über das Marktangebot stützen sich dabei auf die 41 Einträge aus der Befragung, die 131 Interview-Nennungen beschreiben, was im Einsatz ist.

Die Ursache liegt in einer Marktlogik, die ohne klaren Auftraggeber versagt. Der Kopplungsschicht fehlt der Käufer. Ein Produkt braucht eine Stelle, die es beschafft, betreibt und verantwortet.



„Die Daten sind da – es fehlt die ermächtigte Instanz mit Ownership und rechtlicher Grundlage, sie zusammenzuführen.“

Dennis Ruf • Senior Vice President Sales Defense, conet

Nach der Krise bricht das Angebot ein zweites Mal ab. Zwei von 172 Lösungen betreffen den Wiederanlauf. 62 zielen auf die akute Lage, 45 auf die Vorsorge, 52 wirken über mehrere Phasen. Für elf Lösungen ist keine Phase erkennbar. Vorsorge lässt sich planen und ausschreiben. Die akute Lage erzeugt Dringlichkeit und Geld. Der Wiederanlauf beginnt mit dem Ende der öffentlichen Aufmerksamkeit.

Der Markt liefert Sensoren und Werkzeuge, die Verdichtung dazwischen bleibt offen.

Versucht wird die Verdichtung durchaus – nur jeweils für einen Ausschnitt. Der Bundesverband Güterkraftverkehr arbeitet mit dem Bundesamt für Logistik und Mobilität an einem Ressourcenregister, ein Fahrzeugkataster existiert bereits. Was fehlt, ist ein Verzeichnis darüber, wer über welche Ressourcen verfügt.

Für die Beschaffung folgt daraus eine wichtige Regel: Angebotsdichte zeigt Wettbewerb, keinen vorrangigen Bedarf. Führungs- und Entscheidungsunterstützung gilt offiziell als Lücke und ist zugleich das drittstärkste Feld im Marktangebot. Eine anbietergetriebene Auswahl investiert daher leicht am entscheidenden Engpass vorbei.

PHASEN

Der Wiederanlauf hat keinen Markt

	Erkennen	Entscheiden	Handeln	Durchhalten	SUMME
Davor	21	6	5	13	45
Dabei	13	4	35	10	62
Danach	1	0	0	1	2
Querschnitt	52 Lösungen wirken phasenübergreifend				52

Elf Lösungen tragen keine Phasenzuordnung. Basis: 172 erfasste Lösungen. Die Spalte Entscheiden trägt über alle Phasen 18 Lösungen – die schwächste der vier.

Abb. 5.6: Lösungs-Datenbank GSÖ 2030

Fünf Sektoren suchen dasselbe Gesamtbild

Fünf Sektoren melden unabhängig voneinander fehlende Übersicht.

In der Logistik gibt es keine Güterleitzentrale mit vollständiger Transparenz. Hanno Friedrich von der Kühne Logistics University weist darauf hin, dass die Unternehmen ihre eigenen Flotten in Echtzeit verfolgen – kein staatlicher Akteur führt diese Daten zusammen, und die Firmen dürften sie aus Wettbewerbsgründen nicht teilen.

Im Gesundheitswesen fehlt die zentrale Übersicht über freie Krankenhausbetten, Operationskapazitäten und Spezialfähigkeiten. Leif Erik Sander von der Charité nennt Echtzeittransparenz über die eigenen Ressourcen den größten Hebel.

Im Schienenverkehr bleiben die Lagebilder des Regionalverkehrs fragmentiert. Martha Klare von der Universität der Bundeswehr München nennt für Betreiber kritischer Infrastruktur vier fehlende Angaben: Zustand von Strom, Wasser, Kommunikation und Transport, verfügbare Ressourcen und einsatzfähiges Personal. Mehrfachplanungen bleiben unsichtbar, eine Person kann zugleich Reserve- dienst und Feuerwehr zugeordnet sein. In der Wirtschaft endet der Blick in die Lieferketten häufig bei direkten Zulieferern. Nach Kai Hoberg von der Kühne Logistics University kennen die meisten Unternehmen noch die erste Stufe, die zweite nur teilweise, die dritte kaum.

Ein Detail aus dem Krisenstabserlass zeigt den Rückstand: Die Anlage trägt bis heute den Titel „Lagebericht“ und besteht im Kern aus einem Blatt Papier, das ausgefüllt und per E-Mail versandt wird.



„Ich bin wirklich nicht die IT-Affine – aber ein digitales Lagebild ist für mich schon sträflich überfällig.“

Marlis Cremer • Deutsches Rotes Kreuz

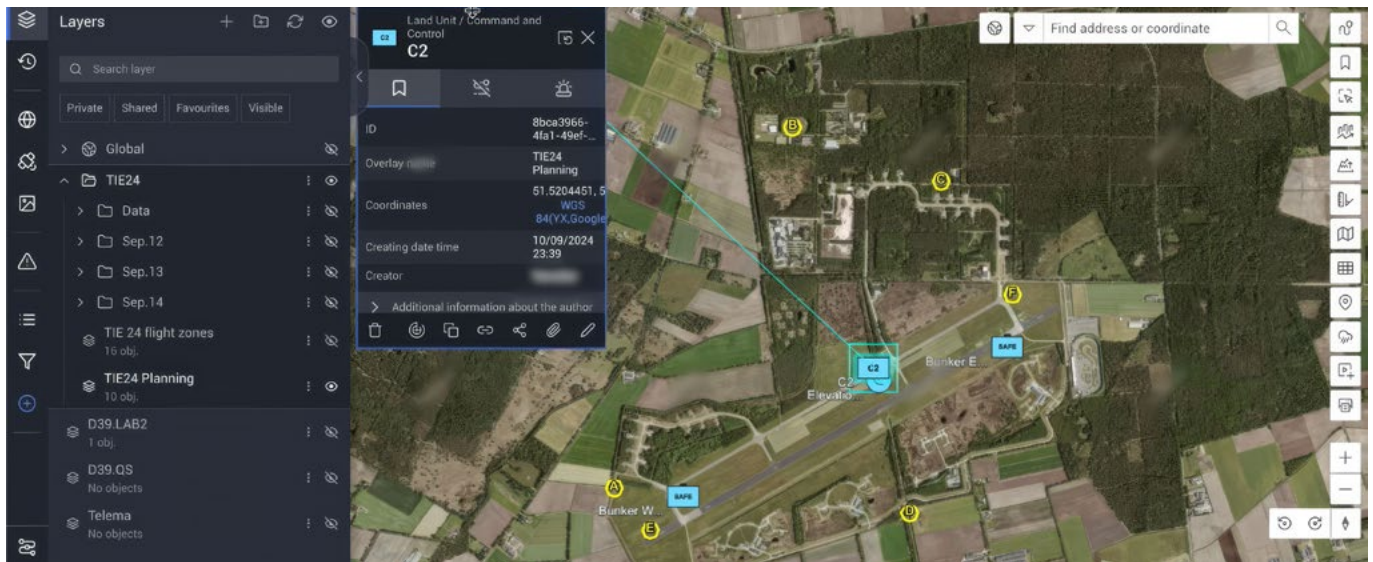
An der Technik liegt es nicht. Sven Hallbauer von der EWERK Group hält ein Lagebild in Echtzeit samt Historie und Abweichungsanalyse für technisch unproblematisch. Sven Weizenegger vom Cyber Innovation Hub der Bundeswehr benennt, woran es stattdessen liegt: an der Klassifizierung und der Frage, wer was sehen darf.

Der Markt kann diese Lücke allein nicht schließen. Die verbindende Aufgabe muss institutionell vergeben werden. Bis dahin entstehen weitere Insellösungen, die jeweils für sich funktionieren.

Selbst funktionsfähige Lösungen gelangen kaum in die Fläche. Dass es anders geht, zeigt ein Fall unter Kriegsbedingungen.

5.5 – DAS GEGENBEISPIEL

Übertragbar ist die Bauweise, nicht das System



Delta · Ukraine, seit August 2022

Die Ukraine betreibt bereits jene Kopplungsschicht, für die in Deutschland ein belastbares Angebot fehlt. Delta führt seit August 2022 Satellitenbilder, Drohnenaufklärung, nachrichtendienstliche Erkenntnisse, offene Quellen und Meldungen vor Ort zusammen. Seit Februar 2023 betreibt es der Staat.

Delta entstand nicht am Reißbrett. Aus vielen einzelnen Anwendungen führte das Verteidigungsministerium ein System of Systems zusammen, die Rechte liegen beim Ministerium. Hans-Martin Zimmermann von Airbus Defence and Space nennt das ein Korrektiv zu den Ein-System-Vorstellungen, die in den Gesprächen dominieren. Damit ist Delta das Gegenmodell zur vollständig vorab entworfenen Architektur, die Abschnitt 5.1 als dritte deutsche Antwort beschreibt.

Entscheidend ist die Bauweise. Delta zentralisiert nicht: Die Oblaste bleiben für ihren Bereich verantwortlich, das System verbindet sie – keine Steuerung aus Kiew. Tobias Schönherr von der Bundespolizei hebt genau das hervor und sieht darin eine Ähnlichkeit zur föderalen Logik Deutschlands.

Der Gewinn liegt in der Geschwindigkeit. Zimmermann beschreibt die Leistung als Echtzeitfusion lokaler Daten aus Bürger-, Polizei- und Drohnemeldungen. Jens Dommel von AWS beziffert den Effekt: Die Cloud-Nutzung habe eine Lageanalyse von einer Stunde auf wenige Minuten verkürzt. Die Angabe stammt aus einem eigenen Kundenprojekt und ist nicht unabhängig geprüft.

Zwei Preise sind mitzudenken. Viele Quellen verschärfen die Vertrauensfrage: Für Sicherheitsorganisationen stellt sich damit die Frage, auf welche Informationen sie ihre Lagebeurteilung stützen. Zerstörte

Bodennetze machten Satelliteninternet nötig – und die Ukraine damit abhängig von einem privaten amerikanischen Anbieter.



„Es wird schwierig zu wissen, wem ich vertrauen kann.“

Ralph Michel • Global Head of Sales Defence & Space, [secunet](#)

Nicht alles daran ist übertragbar. Benedikt Meng von infodas hält Delta für ein Konstrukt, das genauere Betrachtung verdient, nennt die Sicherheit aber als größtes Problem der browserbasierten Plattform mit ihren vielen externen Anbindungen. Vom ukrainischen Beschaffungs-App-Store rät er ausdrücklich ab: Eine an Computerspiele erinnernde, von Spieleentwicklern gebaute Lösung möge für sehr junge Drohneneinheiten intuitiv sein – für den deutschen Kontext taugt sie nicht.

Der Krieg setzt andere Regeln und ein anderes Tempo. Delta belegt die Machbarkeit einer Kopplungsschicht unter härtesten Bedingungen. Nötig sind dafür ein Mandat, offene Schnittstellen, geprüfte Quellen und ein Kanal für zivile Meldungen.

EXKURS · BAUPLAN FÜR DAS PERFEKTE LAGEBILD

Der Angriff kommt vor dem Behördenfax

Links nach recht: Erik Zahn, Tamino Müller, Aaron Emde, Kpt. z S Dr. Dr. Robert Koch

Ein Wasserwerk meldet den Ausfall aller Pumpen. Als Ursache nennt es fehlenden Strom. Der regionale Netzbetreiber meldet zur gleichen Zeit stabile Versorgung. Heute können beide Angaben getrennte Behörden erreichen und als zwei Wahrheiten liegen bleiben.

In der Arbeit „Perfektes Lagebild: Echtzeitüberwachung von Bedrohungen kritischer Infrastrukturen“ löst der Widerspruch Alarm aus. Das System markiert einen möglichen Manipulationsversuch oder Sensorfehler und hält die Meldung aus dem nationalen Lagebild heraus. Das Papier entstand im Programm Hacking4Defense, das an der Universität der Bundeswehr München Verteidigungsprobleme mit Methoden der Gründerszene bearbeitet. Drei Studenten — Aaron Emde, Tamino Müller und Erik Zahn — führten dafür 111 Experteninterviews und Fachgespräche. Als Problemsponsor begleitete Kapitän zur See Dr. Dr. Robert Koch die Arbeit.

Hybride Angriffe verbinden Cyberattacke, Sabotage und Informationsoperation. Sie laufen in Stunden. Das Recht rechnet mit Meldungen nach 24 oder 72 Stunden. Der Angriff erreicht die nächste Infrastruktur oft vor dem ersten Behördenfax.

Rohdaten bleiben beim Betreiber. Eine lokale Middleware übersetzt Sensordaten in standardisierte Ereignisobjekte und versieht sie mit einer digitalen Signatur. Die erste Stufe beschreibt den Vorfall, die zweite verdichtet mehrere Vorfälle zu Abhängigkeiten. IP-Adressen, Softwarestände und Schwachstellen bleiben in der Anlage.

Im Regelbetrieb werden die Objekte in festen Abständen abgerufen. Überschreitet ein Ereignis einen Schwellenwert, folgt die sofortige

Übermittlung. Reißt die Verbindung ab, speichert die lokale Komponente die Meldungen und synchronisiert sie später.

Auch der Rückweg ist gebaut. Wer mehr als die Pflichtmeldung liefert, erhält Warnprodukte zurück. Open Source Intelligence, kurz OSINT, bezeichnet die Auswertung öffentlich zugänglicher Quellen: Satellitenbilder, Verkehrs- und Wettermeldungen, Netzlasten, Schwachstellenregister und Hinweise aus dem Darknet. Sprachmodelle sortieren die Masse, Analysten bewerten Quellen und Zusammenhänge. Daten gegen Warnvorsprung: Das schafft einen Anreiz zur Kooperation und eine Prüfebene gegen Falschdaten.

Für den Krisenfall beschreiben die Autoren drei Eskalationsstufen. Abrufzyklen verkürzen sich, Warnungen erhalten Vorrang, zusätzliche Datenzugriffe werden vorbereitet. Als möglichen Rechtshebel nennen sie die Europäische Datenverordnung, den Data Act. Das Nationale Cyber-Abwehrzentrum soll zeitweise eine begrenzte Führungsbefugnis erhalten. Die Studie gibt diese institutionelle und rechtliche Empfehlung als Position der drei Autoren wieder.

Der Bauplan setzt bei vorhandenen Behörden, Daten und Netzen an. Seine Leistung liegt in der Kopplung: Aus Meldungen werden geprüfte Lageobjekte, aus Lageobjekten Wirkzusammenhänge, aus Wirkzusammenhängen Entscheidungen. Gehackt wird die Zeit, die heute zwischen Signal und Handlung verloren geht.

5.6 – DER TRANSFORMATIONSPFAD

Erst Regeln und Rechte, dann Technik

Wer das digitale Rückgrat bis 2030 tragfähig machen will, muss acht Anforderungen erfüllen, bevor die erste Ausschreibung startet. Sie verdichten, was die vorangegangenen Abschnitte gezeigt haben – genannt von denen, die diese Systeme bauen, beschaffen und nutzen.

Eine verbindliche Datensprache. Vor der Verbindung muss geklärt sein, was die Angaben bedeuten. In der Pandemie war bereits uneinheitlich definiert, wann ein Bett als frei gilt. Abweichende Erstmeldungen führen zu Fehlentscheidungen.

Offene Schnittstellen als Vergabebedingung. Ein Angebot ohne sie scheidet aus. Geschlossene Systeme belohnen den Anbieter, nur die Ausschreibung kann das ändern.

Eine Anschlusspflicht. Estland setzte seine Schnittstellenarchitektur durch, weil sich alle beteiligen mussten. Der europäische Standard für Behördenbreitband ist beschlossen und erprobt, in der Fläche jedoch kaum angekommen. Es fehlt an Verbindlichkeit.

Abgestufte Zugriffsrechte. Ein System muss Daten verschiedener Sicherheitsbereiche verbinden und zugleich den sichtbaren Ausschnitt je Rolle begrenzen. Feuerwehr und Bundeswehr benötigen unterschiedliche Informationen.

Prüfbare Einstufungen. Eine hohe Einstufung kann die Weitergabe eines Lagebildes technisch verhindern. Jede Schutzstufe braucht daher eine Begründung und ein geregeltes Zugriffsmodell. Zugleich fehlen Systeme mit Anschluss an die Partner der Nordatlantischen Allianz.

Fortlaufende Prüfung. Eine einmalige Zulassung reicht nicht mehr. Kontinuierliche Kontrolle und schnelle Reaktion sind technisch möglich, organisatorisch jedoch ungewohnt.

Ausfallsicherheit der Systeme. Direktmodus im Digitalfunk und lokal vorgehaltene Lagedaten sichern den Betrieb beim Ausfall der Datenetze.

Zykluszeit als Abnahmekriterium. Neben der Vollständigkeit muss die Dauer von der Beobachtung bis zur Wirkung gemessen werden. Ohne diese Kennzahl wird am operativen Bedarf vorbei optimiert.

Das Regelwerk muss vom Auftrag her entworfen werden. Über allen acht Punkten steht diese Grundentscheidung: Regeln müssen den

Auftrag ermöglichen und seine Risiken begrenzen. Vorgaben, die den Zugang zu entscheidender Technik versperren, erzeugen neue Schwachstellen. Jens Dommel von AWS fordert genau das.

Die Grenze liegt in der Bündelung sensibler Angaben. Ein zentrales Verzeichnis von Schwachstellen wäre bei einem Datenleck ein wertvoller Fund für Angreifer.

Die Reihenfolge lautet: erst Begriffe klären, dann Beteiligung verbindlich machen, anschließend Technik beschaffen. Ralph Michel von secunet hält die technischen Mittel weitgehend für vorhanden. Entscheidend seien Datenqualität, geklärte Zuständigkeiten und eingeübte Praxis.

Jede Ebene liefert ihren Teil. Bund und Ressorts legen Datensprache und Verbindlichkeit fest, Länder und Kommunen liefern operative Angaben, Anbieter offene Schnittstellen. Ansgar Kaltwasser von CGI empfiehlt vertraute Werkzeuge, um den Ausbildungsaufwand zu senken.

Die Handlungsfelder mit Zeitbändern führt Kapitel 7. Was hier steht, ist die Voraussetzung dafür, dass sie greifen.

06

TechKompass

Fähigkeitsbeiträge zum Sicherheits- ökosystem 2030

6.0 – DER MARKT

Wirkung ordnet den Markt



Der Markt sortiert Cloud, Funk, Sensorik und Cybersicherheit nach Produktwelten. Welche Beiträge gewinnen Zeit, verbessern Entscheidungen, bringen Wirkung in die Fläche und halten den Betrieb aufrecht? Der TechKompass zum gesamtstaatlichen Sicherheitsökosystem dreht die Blickrichtung um.

Der erfasste Lösungsbestand ist groß genug für ein Muster und klein genug für sichtbare Lücken. Reife, Skalierbarkeit und Hemmnisse werden deshalb nach Wirkung geordnet, viel Angebot kann geringe Systemreife verdecken. Erst diese Landkarte macht die folgenden Felder vergleichbar. → [6.1](#)

Früher erkennen verlangt Sensorfusion und eine belastbare Verdichtung heterogener Quellen. Dazu können auch Meldungen aus der Bevölkerung gehören, sobald ein Schwellenwert unabhängiger Bestätigungen ihre Verlässlichkeit prüft. Der Weg führt vom einzelnen Signal zum gemeinsamen Lagebild. → [6.2](#)

Schneller und besser entscheiden verschiebt den Schwerpunkt zu Künstlicher Intelligenz. KI-Agenten, also spezialisierte Softwareeinheiten mit klaren Rollen, können parallel Hypothesen prüfen. Ihre Qualität hängt an Datenzugang, Datenqualität und einer menschlichen Entscheidung am Ende der Kette. Technik verkürzt Entscheidungszeit, ohne Verantwortung zu automatisieren. → [6.3](#)

Wirksamer handeln braucht eine verlässliche Verbindung zwischen Entscheidung, Wirksystem und Informationsraum. Dazu gehört auch Manipulationsschutz: Desinformation muss erkannt, eingeordnet und in einer vorbereiteten Kommunikationsarchitektur beantwortet

werden. Entscheidend ist Technik, die aus einer Entscheidung belastbare Wirkung macht. → [6.4](#)

Länger durchhalten heißt, kritische Funktionen unter anhaltender Störung weiterzuführen und den Wiederanlauf vorzubereiten.

Technik trägt dazu bei. Personal, Vorräte, Ersatzteile, Rückfallverfahren und geübte Prioritäten entscheiden über die tatsächliche Fähigkeit. Technischer Beitrag und Durchhaltefähigkeit sind zweierlei. → [6.5](#)

Orchestrierung, also verbindliche Koordination über Organisationsgrenzen, lässt sich kaum als Einzelprodukt kaufen. 19 der 172 erfassten Lösungen tragen einen Orchestrierungsbezug. Der Bestand besteht vor allem aus Konzepten, Programmen und Systemen. Die verbindende Fähigkeit braucht ein Mandat, kein Produkt. → [6.6](#)

Damit aus Einzelangeboten ein digitales Rückgrat wird, muss Beschaffung Wirkung zum Auswahlkriterium machen. Offene Schnittstellen, kommunale Reichweite, Kostenmodelle, Haftung und eine fortlaufende Marktübersicht bestimmen, ob aus technischer Reife Einsatzfähigkeit entsteht. Damit wird der TechKompass zum Auftrag an Beschaffung und Anbieter. → [6.7](#)

6.1 – DIE LÖSUNGSLANDSCHAFT

Wirksamkeit muss zum Auswahlkriterium werden

Die genannten Lösungen ergeben ein Inventar wachsender Handlungsfähigkeit. Kommunikationssysteme, Lagebilder, Sicherheitsplattformen, Warnsysteme. Eine Auflistung allein führt durch keine Krise. Drei Fragen führen weiter: Was bietet der Markt, wie reif sind die Angebote und warum kommen sie nicht in die Fläche?

Für die Orchestrierung wurde kein beschaffbares Produkt genannt, zugleich ist sie die meistgenannte Bruchstelle der Praxis.

Drei Quellen tragen dieses Kapitel. Die Interviews liefern die 172 erfassten Lösungen – dort berichten die Gesprächspartner über ihren Einsatz, selten über Reifegrade. Die Online-Befragung unter 72 Teilnehmenden aus Technologieunternehmen, Systemintegration, Forschung, Beratung, Bedarfsträgern und Betreibern erfasst Reife, Skalierbarkeit und Hemmnisse. Und die 13 Beiträge der Studienpartner ab Seite 76 zeigen, was einzelne Anbieter konkret leisten.

Das Angebot bildet das Bedrohungsbild kaum ab. Cyberangriffe und hybride Bedrohungen nennen die Befragten mit zusammen 38 Prozent als häufigste Anwendungsfälle. Im Angebot machen Cyber- und Sicherheitslösungen sieben Prozent aus.

Das Angebot deckt den Anfang der Krise ab, kaum jedoch ihr Ende. 42 Prozent der Lösungen zielen auf die Zeit vor einer Lage, 50 Prozent auf die Lage selbst. Auf Resilienz und Wiederanlauf entfallen sechs Prozent. Es ist die einzige Funktion, deren Bedarf das Angebot übersteigt. Das Muster zeigt sich auch rückblickend: Für die systematische Auswertung vergangener Krisen bietet der Markt nichts an. Im Partnerworkshop im Juni 2026 fiel dafür der Begriff Krisendemenz.

Zwei Akteursgruppen fehlen im Angebot. Die Bevölkerung kommt nicht vor, obwohl 47 Prozent der Befragten Bürgereinbindung als Nachholbedarf nennen. Auch die Wirtschaft jenseits der regulierten kritischen Infrastruktur fehlt – der Logistiker, der im Ernstfall Ausweichstrecken kennt und Versorgung fährt, ist in keiner Lösung vorgesehen.

Die wirksamsten Lösungen liegen an den Schnittstellen. Kommunikation und Vernetzung ist mit 39 Prozent der größte Lösungstyp, ein Massenmarkt. Die höchsten Wirkungsbeiträge tragen die selteneren Lagebild- und Schnittstellenlösungen – allen voran RessüLa, die ressortübergreifende Lage zwischen zivilen und militärischen Systemen. Der Markt wächst vor allem in großen Segmenten, der Wirkungsbeitrag entscheidet kaum.

Mehr Lösungen schließen die Lücke nicht

Die Befragung präzisiert den Befund. Trägt man für jede der sieben Fähigkeiten Reifegrad, Handlungsbedarf und Zahl der Lösungen ab, entsteht das Bild unten: Ausgerechnet Kommunikation und Vernetzung, die am häufigsten geforderte Fähigkeit, bündelt mit 23 Nennungen das meiste Angebot – bei der niedrigsten Reife und dem höchsten Bedarf. Keine Fähigkeit erreicht die Zielzone.

Die Daten erlauben zwei Diagnosen: Viel Angebot bei geringer Reife weist auf ein Skalierungsproblem. Wo das Angebot gering bleibt, etwa bei Cyber und digitaler Resilienz, fehlt die Fähigkeit selbst.

Die Befragten benennen die Skalierungshürden selbst: 55 Prozent nennen die Beschaffung, 42 Prozent unklare Zuständigkeiten und Steuerung. Dahinter stehen zwei unterschiedliche Probleme. Wer die Beschaffung nennt, hat im Schnitt die reifsten Lösungen – fertige Produkte, die nicht durch die Vergabe kommen. Wer unklare Verantwortlichkeiten nennt, weist deutlich geringere Reifegrade auf. Die Beschaffung bremst, was fertig ist. Unklare Steuerung verhindert, dass Lösungen entstehen.

Interoperabilität nennen nur 13 Prozent als größtes Hemmnis. Das heißt nicht, dass sie gelöst wäre. Als die Partner der Studie die Befunde im Juni 2026 gewichtet haben, landete sie auf dem ersten Platz – vor allen Prozentwerten. Sie ist das Scharnier, an dem die Skalierung hängt. Ihre Bedeutung zeigt sich, sobald Beschaffung und Steuerung geklärt sind.

Die Diskussion nahm eine unerwartete Richtung. Interoperabilität gilt üblicherweise als Aufgabe der öffentlichen Seite: einheitliche Standards, klare Verantwortlichkeiten, verbindliche Schnittstellen. Die Partner wiesen auch auf Hindernisse auf Anbieterseite hin: Schnittstellen dienen häufig der Abgrenzung, Offenheit berührt das eigene Geschäftsmodell. Silos entstehen auf beiden Seiten des Tisches.

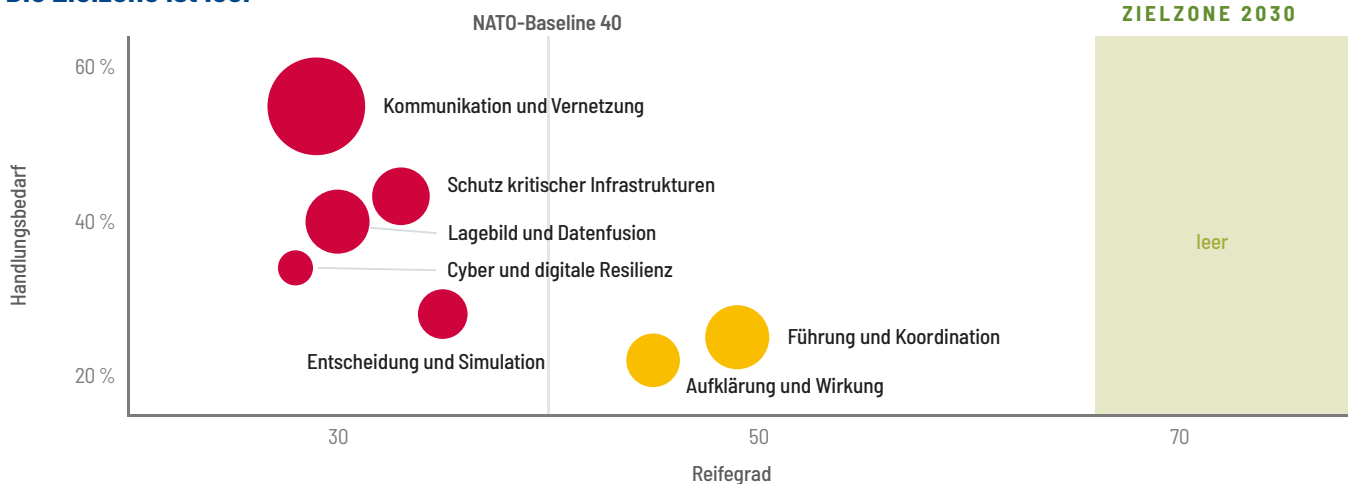
Neun von zehn Lösungen halten die Befragten für bis 2030 skalierbar. Die technische Machbarkeit erklärt den Mangel in der Fläche daher kaum.

Internationale Beispiele zeigen, dass sich die Lücke schließen lässt. Estland hat mit X-Road eine Schnittstellenarchitektur durchgesetzt, an die 99 Prozent der staatlichen Datenbankdienste angeschlossen sind – der Anschluss war verpflichtend. In den Vereinigten Staaten wurde FirstNet aufgebaut und ausgerollt. Europa erprobte das Konzept mit BroadWay und beschloss die Umsetzung, in der Fläche kam sie bislang nicht an. Entscheidend ist die Verbindlichkeit.

Die folgenden fünf Abschnitte untersuchen die Felder einzeln: Was ist heute beschaffbar und welche Bausteine fehlen?

REIFE UND BEDARF

Die Zielzone ist leer



Blasengröße = Zahl der genannten Lösungen · fünf Fähigkeiten liegen unter der NATO-Baseline, zwei darüber, keine in der Zielzone

Langformen: Gemeinsames Lagebild und Datenfusion · Führung und Einsatzkoordination · Kommunikation und sichere Vernetzung · Schutz und Resilienz kritischer Infrastrukturen · Entscheidungsunterstützung und Simulation · Aufklärung, Sensorik und Wirkung · Cyber und digitale Resilienz

Abb. 6.1: GSÖ-Befragung unter Technologieanbietern und Anwendern, N = 72

6.2 – FRÜHER ERKENNEN

Sensordaten müssen ein gemeinsames Bild ergeben



Früher erkennen heißt: Signale aufnehmen, verdichten und weitergeben, bevor eine Lage kippt. Die Informationen müssen Sektor- und Organisationsgrenzen überschreiten und Entscheidungen tragen.

Mit 56 der 172 erfassten Lösungen ist dies das dichteste Feld im Bestand, 33 Lösungen sind im Betrieb. Sensorik, Warnsysteme, Lagebildsysteme: Hier hat Deutschland gebaut. Zwei Lücken bleiben – an der Grenze zwischen physischer und Cyberlage, und bei der Kopplung heterogener Sensorik.

Am weitesten fortgeschritten ist die Zusammenführung von Sensordaten. In Rostock führt die Bundeswehr Daten von See bis Weltraum zu einem einheitlichen Lagebild zusammen. Sven Weizenegger vom Cyber Innovation Hub beschreibt den Zweck: ein Lagebild bereithalten, statt es erst nach Eintritt der Lage zusammenzustellen.

Der Verbund endet an der Grenze zwischen physischer Lage und Cyberlage. Das Fraunhofer FKIE hat beschrieben, wie eine gemeinsame Darstellung aussähe – Drohnerdetektion, Desinformationskampagnen, Cyberangriffe und Verkehrsdaten in einem Bild. National gibt es dafür kein Vorhaben, nur eine NATO-Ausschreibung.

Auch zwischen den Sensoren fehlt die Kopplung. Für die Anbindung heterogener Systeme stehen die NATO-Schnittstelle SAPIENT und der erweiterbare Standard STANAG 4676 bereit. Beschaffbar ist bislang keine dieser Optionen.

Eine Datenquelle bleibt dabei ungenutzt: die Bevölkerung. In der Ukraine fließen Beobachtungen von Bürgern, Polizei und Drohnen in ein gemeinsames Lagebild ein. Erst ausreichend bestätigte Meldungen gelangen in die operative Nutzung.

Dasselbe Muster wiederholt sich eine Ebene höher. Der Anlauf der kommunalen Spitzenverbände für ein bundesweit einheitliches digitales Lagebild scheiterte an den Ländern.

Technik ist dabei kaum der Engpass. Das zeigt ein Beispiel von Marlis Cremer vom DRK Düren. Im Umfeld der Weltmeisterschaft 2006 und des Papstbesuchs entstand in Deutschland ein digitales Lagebildsystem. Die Niederländer kauften es und nutzen es seit 20 Jahren.

Beide Lücken haben ein Angebot. Auf die Grenze zwischen den Sicherheitsdomänen antwortet infodas: Wo die Einstufung ein genaues Lagebild unteilbar macht, verbindet das Unternehmen die Domänen. Auf die fehlende Kopplung heterogener Sensorik antwortet Airbus mit einem bodengebundenen System für die nationale Luftlage und einem darauf aufsetzenden Führungssystem für beliebige Sensoren und Effektoren.

infodas

Zwei Lagebilder, kein Übergang

infodas IM SICHERHEITSÖKOSYSTEM

Ein Lagebild entsteht erst, wenn Daten die Domänengrenze überschreiten dürfen

- » Sichere Übergänge zwischen getrennt geführten Sicherheitsdomänen
- » Abgestufter Zugang zum militärischen Lagebild statt Vollzugriff
- » Zugelassen bis GEHEIM, EU SECRET und NATO SECRET
- » Cross-Domain-Praxis für Streitkräfte, Nachrichtendienste und KRITIS



Eine hybride Lage mit Sabotage trifft Deutschland womöglich genau dann, wenn der Großteil der Bundeswehr an der NATO-Ostflanke steht. Im Inland bliebe dann, wie Benedikt Meng es formuliert, nur noch der Heimatschutz. Die Frage ist, ob die technischen Möglichkeiten bestehen, diese Lage gemeinsam zu kommunizieren.

Übersetzt wird heute von Hand. Zivile und militärische Lagebilder laufen getrennt. Wo sie zusammenkommen müssten, geschieht das über Personen statt über Systeme. Meng kennt das aus dem Nachrichtenbereich: Schon die Querbeziehung zwischen zwei Landespolizeien ist schwierig, weil Unsicherheit herrscht, was mit wem geteilt werden darf.

Nicht jeder muss alles sehen. Zivile Stellen lassen sich nicht einfach an das militärische Lagebild anbinden, weil dort vieles geführt wird, das nicht jeder sehen muss. Nötig ist kein Vollzugriff, sondern eine kontrollierte Abstufung: welche Information die Domäne verlässt und welche in ihr bleibt.

infodas baut den Übergang. Der Kern ist die Fähigkeit, ein höher und ein niedriger eingestuftes System zu verbinden, die im Standardzustand getrennt sind – militärisch wie zivil, zugelassen bis GEHEIM, EU SECRET und NATO SECRET. Diesen Datenaustausch leistet das Unternehmen seit Jahren für Streitkräfte und Nachrichtendienste, zunehmend auch im KRITIS-Bereich. Dazu Sicherheitskonzepte, Beratung und Arbeiten daran, KI in Hochsicherheitsumgebungen nutzbar zu machen.

Die Reziprozitätslücke bremst die Fläche. Das KRITIS-Dachgesetz regelt vor allem, was der Betreiber dem Staat schuldet, kaum, was er vom Staat erwarten kann. Ohne Rückkanal zum gesicherten Lagebild hat er wenig Anreiz, mehr beizutragen als vorgeschrieben. Der technische Übergang allein genügt nicht.

Zwischen Nachweis und Entscheidung. Der Engpass liegt nicht in der Technik, sondern im ressortübergreifenden Mandat, in der Entscheidung, eine nachgewiesene Fähigkeit zu skalieren, und im Budget für die Fläche. Meng hält eine skalierte Umsetzung bis zum Zieldatum 2029 für machbar – vorausgesetzt, die Kosten trägt nicht der Verteidigungshaushalt allein.

REFERENZLÖSUNGEN

Sicherer Domänenübergang – zugelassen bis NATO SECRET

infodas verbindet Systeme unterschiedlicher Einstufung, die im Standardzustand getrennt geführt werden. Die Übergänge sind bis GEHEIM, EU SECRET und NATO SECRET zugelassen und seit Jahren für Streitkräfte und Nachrichtendienste im Einsatz, zunehmend auch bei Betreibern kritischer Infrastruktur.

In einem ressortübergreifenden Lagebildvorhaben des Bundes ist die Fähigkeit über den Demonstrator hinaus erprobt: Ein gemeinsames Lagebild über unterschiedliche Einstufungen hinweg und ohne Medienbruch ist technisch nachgewiesen; an der Verstetigung wird gearbeitet.

Mengs Schluss daraus: Die technische Machbarkeit steht. Was fehlt, ist die Entscheidung zu skalieren – und die Bauform dafür ist eine Orchestrierungs-Zwischenschicht, die von der Einspeisung lebt und ein Kontinuum zwischen offenem Internet und eingestuftem Domänen herstellt.

Drei Hebel – einfach machen

1. Eingriffsschwellen und Attribution vor der Krise klären, nicht im Ernstfall.
2. Die erprobte Lagebildfähigkeit skalieren – eine Entscheidung, kein Technikproblem.
3. Rückkanal zu KRITIS-Betreibern öffnen: Lagebildzugang statt Meldepflicht.

„Dann bleibt das halt so eine PowerPoint-Schlacht, wo der Polizeihauptkommissar in den Gefechtsstand einer Heimatschutzkompanie geht und zu übersetzen versucht, was er sieht.“

Benedikt Meng • Leiter Business Development & Strategie, infodas

AIRBUS DEFENCE AND SPACE

Das Lagebild ist da. Teilen lässt es sich nicht.

AIRBUS IM SICHERHEITSÖKOSYSTEM

Die Lücke sitzt nicht in der Sensorik, sondern im Übergang

- » Nationale Luftlage. Führung der bodengebundenen Luftverteidigung sowie Drohnenabwehr
- » Führungssysteme mit flexibler Anbindung geeigneter Sensoren und Effektoren
- » Datenaustausch über Sicherheitsgefälle über Gateways
- » Offene Architektur auf bestehenden NATO-Standards statt neuer Instanz



Ein Drohnenschwarm über einer Bundeswehr-Liegenschaft, daneben ein Industriegebiet mit Umspannwerk, in der Nähe ein Flughafen. Schlagartig sind Bundeswehr, Landespolizei, Flugsicherung, KRITIS-Betreiber, Industrie, Bürger und Lokalpolitik beteiligt – jeder in seiner eigenen Organisation. In der Theorie gibt es passende technische Lösungen. In der Praxis, sagt Dr. Hans-Martin Zimmermann, endet es bei Drehstuhl und Telefon.

Der Operateur weiß nicht, ob er darf. Vor dem Schirm steht zuerst die Zuständigkeitsfrage: Gilt der Anflug der Liegenschaft oder dem Umspannwerk nebenan? Jugendstreich oder Angriff? Einzerner oder ausländischer Staat – woran sich jeweils andere Zuständigkeiten knüpfen. Gefordert ist abgestimmtes Handeln, nicht isoliertes Agieren.

Erkennen ist nicht das Problem. Ein Sensorverbund aus Radar, Funkaufklärung, Elektrooptik, Infrarot und Akustik erzeugt ein sehr genaues lokales Lagebild, skalierbar über Standorte. Die Schwierigkeit beginnt beim Teilen: Sicherheitsanforderungen verbieten die einfache Herausgabe, für die digitale Direktübergabe fehlt die Interoperabilität. Das eingestufte Lagebild bleibt im eigenen System, die Freigabe des Wirkmittels im besten Fall eine lokale Reaktion.

Die Übereinstufung verhindert nahtlose Vernetzung. Je höher ein Lagebild über die Ebenen aggregiert wird, desto sensibler wird es – und im militärischen Bereich wird aggregiert oft sehr schnell sehr hoch eingestuft. Die Folge: Andere Akteure haben weder Infrastruktur noch Berechtigung, es zu empfangen und zu reagieren.

Der Beitrag: Luftlage, Führung, Luftverteidigung, Übergänge. Die Fähigkeiten von Airbus liegen in Aufklärung, digitaler Führungsfähigkeit, Luftverteidigung inklusive Counter-UAS, Künstlicher Intelligenz (KI) und Cybertechnologie. Konkret genannt sind ISkyControl als Gehirn des German Improved Air Defence Systems (GIADS) für die nationale Luftlage im Control and Reporting Center (CRC), das Surface-to-Air Missile Operations Center (SAMOC) als Koordinationsfunktion der bodengebundenen Luftverteidigung sowie die Integrated Battle Management Software (IBMS) als Führungssystem angebundener Sensoren und Effektoren. Die Konzerntochter infodas steuert Gateways für den Austausch über Sicherheitsdomänen bei, während Airbus beim BOS-Digitalfunk Systemlieferant ist.

Standards statt neuer Instanz. Gebraucht wird eine offene Architektur mit Gateways, die Daten über Sicherheitsgefälle hinweg kontrolliert austauschbar macht – gestützt auf erweiterbare Standards wie STANAG 4676 und die SAPIENT-Schnittstelle.

REFERENZLÖSUNGEN

GIADS, SAMOC und IBMS

Das GIADS führt die nationale Luftlage im CRC und ist in die NATO-Struktur eingebunden. Darauf bauen SAMOC und IBMS für die bodengebundene Luftverteidigung auf, an die sich Sensoren und Effektoren flexibel anschließen lassen.

Der Wert für ein gesamtstaatliches Sicherheitsökosystem liegt weniger im einzelnen System als in seiner Interoperabilität: Abhängig vom rechtlichen Rahmen, der Bedrohungslage sowie individuellen Anforderungen werden Sensoren und Wirkmittel über definierte Schnittstellen angeschlossen, um eine skalierbare Lösung zu erreichen – vom Objektschutz gegen Drohnen bis hin zur nationalen Luftverteidigung. Bei veränderter Bedrohungslage können Sensoren und Wirkmittel angepasst werden, ohne das Gesamtsystem austauschen zu müssen.

Drei Hebel – einfach machen

1. Einstufungspraxis für aggregierte Lagebilder überprüfen – teilen können statt abschotten.
2. Auf bestehende Standards aufsetzen: STANAG 4676 und SAPIENT erweitern statt neu erfinden.
3. Physische und Cyber-Lagebilder auf allen Ebenen korrelieren.

„Lagebilder müssen geteilt werden, Entscheider befähigt werden – Bedrohung und Reaktion müssen auf allen Ebenen transparent und anpassbar sein“

Dr. Hans-Martin Zimmermann • Leitung Engineering, Defence Digital - Airbus Defence and Space

6.3 – BESSER ENTSCHEIDEN

Kein ziviles Entscheidungssystem im Betrieb



Besser entscheiden heißt: unter Zeitdruck priorisieren, mit unvollständiger Information und ohne die Möglichkeit, auf Vollständigkeit zu warten.

Dieses Feld ist im Bestand am dünnsten besetzt. 18 der 172 erfassten Lösungen zählen darauf ein, vier davon sind Marktangebote. Ihr höchster erreichter Reifegrad ist erprobt. Was betrieben wird, ist militärisch.

Für den Verteidigungsfall existiert mit dem Operationsplan Deutschland ein erprobter Plan. Sven Ambrosy vom Landkreis Friesland fordert ein verbindliches ziviles Pendant, bislang liegt es nur als Forderung vor.

Was ein Plan nicht leistet, muss die Lagebeurteilung erbringen. KI-Agenten sind spezialisierte Softwareeinheiten mit klaren Rollen. Marianne Janik von Google Cloud beschreibt Tausende solcher Agenten, die parallel Hypothesen prüfen und eine Rangfolge möglicher Lageentwicklungen liefern. Was ein Stab nacheinander bearbeitet, läuft so in vielen Strängen zugleich.

Die Agenten sortieren, gewichten und begründen. Verantwortung, Freigabe und Haftung bleiben beim Menschen – Volker Pötzsch vom Kommando Cyber- und Informationsraum schließt automatisierte Entscheidungen ausdrücklich aus. Erklärbare Künstliche Intelligenz legt Quellen, Unsicherheiten und verworfene Hypothesen offen. Der Stab kann eine Empfehlung prüfen und in einen Auftrag übersetzen.

Damit verschiebt sich die Frage von der Technik auf die Daten. Bernd König von Google Cloud verbindet Daten des Deutschen Wetterdienstes,

privater Wetterdienste und des militärischen Geoinformationsdienstes. Eine KI könnte daraus ein Lageentwicklungsbild und tragfähige Anfahrtswege des Technischen Hilfswerks zu einem bedrohten Deich ableiten. Die Quellen bestehen. Der gemeinsame Zugriff fehlt.

In Telekommunikationsnetzen erkennen Systeme Überlastungsangriffe bereits statistisch und könnten automatisiert reagieren. Thomas Tschersich von der Deutschen Telekom verweist auf den Konflikt mit dem Fernmeldegeheimnis. Die Technik ist einsatzbereit, der Rechtsrahmen muss die Eingriffsschwelle festlegen.

Wo Technik und Recht nicht weiterhelfen, bleibt die Übung. In Norwegen und Dänemark üben Wirtschaftsführer jährlich in einem staatlichen Resilienzprogramm. Norbert Ahrend von Arvato Systems nennt es als Beispiel für eingeübte Entscheidungsvorbereitung.

Beide Angebote setzen an je einer der Lücken an. Google Cloud stellt eine physisch vom offenen Netz getrennte Rechenumgebung für Sprachmodelle bereit – die Antwort auf die Frage, wo eine KI in einem eingestuftem Umfeld überhaupt rechnen darf. conet verbindet soziale Netzwerke, elektromagnetisches Spektrum und Cyberlage zu einem dreidimensionalen Lagebild und schließt damit an die Verdichtung an, die 6.2 offenlässt. Beide stehen im Aufbau, ihr Reifegrad ist erprobt, nicht betrieben.

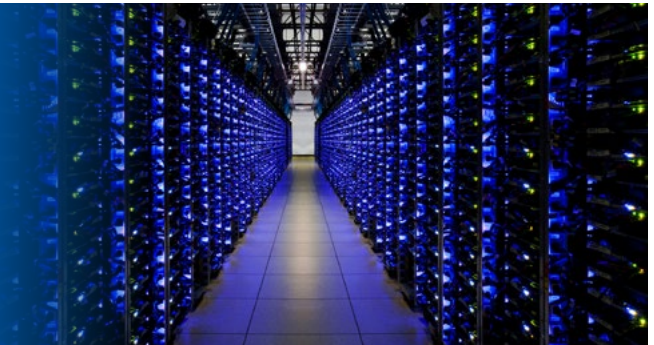
GOOGLE CLOUD

Fähigkeiten im Fokus: Ein Perspektivwechsel

GOOGLE CLOUD IM SICHERHEITSÖKOSYSTEM

Die Fähigkeit ist da. Sie ist nur nicht freigegeben.

- » Souveräne Cloud -Plattform, galvanisch von Betreiber und Netz getrennt
- » Agentische Lagebeurteilung statt weiterer Dashboards
- » Datenqualität als Bedingung, nicht Systembereitstellung
- » Strategischer Partner der BWI, in Verlängerung zum Verteidigungsministerium



Rückblick: Am Abend des 13. Februar 2009 meldete die Tagesschau, die Bundeswehr nehme 150 Liegenschaften vom Netz. Der Conficker-Wurm konnte sich nur ausbreiten, weil ein rechtzeitig gelieferter Patch mangels Zuständigkeit nicht ausgerollt wurde. Bernd König war damals CISO der BWI. Die Technik war da. Die Zuständigkeit nicht.

Überreguliert, nicht unterausgestattet. Es fehle nicht an Fähigkeiten und nicht an Gesetzen, sagt König — im Gegenteil. Die ministerielle Zuständigkeitslogik führe zu faktischer Unzuständigkeit. Ein eigenes Beispiel: Während die Gesellschaft längst startklar ist, verzögern langwierige behördliche Zuständigkeits- und Abstimmungsprozesse beim Geheimschutz die Arbeit.

Jeder baut sein eigenes Dashboard. Trotz zahlreicher neuer Agenturen und Lagezentren entsteht kein übergreifendes Krisenmanagement. Die verlorenen Minuten potenzieren sich im digitalen Raum zu Stunden Vorsprung für einen Angreifer, der sich an Zuständigkeiten nicht hält. Dasselbe zeigt sich als Verantwortungs-Ping-Pong an den Schnittstellen.

Das Problem ist nicht das System, sondern die Datenlage. Beim Bereitstellen von Systemen sei man weit; die Hürde liege in der Datenqualität und in der Beurteilung der Zusammenhänge. Königs Beispiel ist das Wettermodell: Deutscher Wetterdienst, private Anbieter und der militärische Geoinformationsdienst führen getrennte Modelle. Zusammengezogen und KI- ausgewertet ergäbe sich ein Lageentwicklungsbild — bis hin zu den Anfahrtswegen des THW an einen Deich unter Druck.

Der Beitrag: souveräne KI, dort wo die Lücke benannt wurde. Der CIO der Bundeswehr hatte gewünscht, die volle Leistungsfähigkeit des Sprachmodells souverän nutzen zu können; vor einem Jahr ging das technisch nicht. Inzwischen steht Gemini auf der Google Distributed Cloud Air-gapped bereit. Darauf aufsetzend die agentische Auswertung: viele Agenten mit klar umrissenen Rollen, die parallel an Hypothesen arbeiten und eine gerankte Lagebeurteilung liefern.

Der Stolperstein ist nicht technisch. König räumt offen ein, dass der verbleibende Widerstand politischer Natur ist — etwa die Frage, ob

jemand die Betriebsfreigabe versagt. Genau das ist der Befund dieses Abschnitts: Es fehlt nicht an Verfügbarem, sondern an der Entschlossenheit, es in Betrieb zu nehmen.

REFERENZLÖSUNGEN

Google Distributed Cloud Air-gapped — Gemini in der abgeschotteten Umgebung

Die Plattform kapselt eine vollständige Cloud-Umgebung in der Infrastruktur des Nutzers ab. Galvanische Trennung vom Betreiber sichert die Souveränität, galvanische Trennung vom offenen Netz die Resilienz; auf dem logischen Netzwerkpfad ist das System nicht erreichbar.

Neu ist, dass darauf das Sprachmodell in vollem Umfang läuft. Damit adressiert der Beitrag eine Fähigkeitslücke, die der CIO der Bundeswehr selbst benannt hatte — souveräne Nutzung ohne Leistungsverzicht. Stand: verfügbar, nicht in Betrieb; der offene Punkt ist die Betriebsfreigabe.

Drei Hebel — einfach machen

1. Verfügbare Fähigkeiten in Betrieb nehmen.
2. Datenräume behördenübergreifend zusammenführen.
3. Vor der Krise regeln, wer im Krisenfall entscheidet.

„Ein gemeinsames Lagebild, auf das alle gleichzeitig gucken, ohne sich noch anrufen zu müssen.“

Bernd König • Managing Director • Google Cloud Public Sector Deutschland

conet

Welche Änderung führt zu welcher Konsequenz?

CONET IM SICHERHEITSÖKOSYSTEM

Entscheidungen brauchen sichtbare Folgen, nicht mehr Daten.

- » Folgen einer Änderung sichtbar machen, bevor entschieden wird
- » Architekturen statt Einzelvorhaben – Abhängigkeiten offenlegen
- » Betrieb in BSI-C5-geprüften Rechenzentren
- » Vierzig Jahre IT für Bundeswehr und Verteidigungssektor



Fällt ein einzelner Knotenpunkt im Stromnetz aus, entstehen Kaskaden- und Dominoeffekte – nicht nur Haushalte, auch Produktion und Dienstleistung liegen still. Reagiert werden kann aber erst, wenn Führung und Zuständigkeit geklärt sind. Die erste Frage, sagt Dennis Ruf, ist immer dieselbe: Wer ist eigentlich im Lead?

Vier Felder, an denen es bricht. Dennis Ruf ordnet das Problem in vier Handlungsfelder: Schnittstellen und Zuständigkeit, Lagebild und Information, Entscheidung und Umsetzung, Durchhaltefähigkeit und Resilienz – und das immer über Bund, Länder und Kommunen. Die föderale Struktur erschwert die Rollenverteilung; bei Entscheidung und Umsetzung kommen juristische Blockaden und lange Abstimmungswege hinzu.

Die Daten sind da. Die Instanz fehlt. Das Hindernis liegt für Kai Drücker nicht in der Technik. Die Daten liegen an verschiedenen Stellen längst vor; es geht darum, sie zusammenzuführen. Dass das scheitert, ist dieselbe Hürde wie bei der Registermodernisierung – warum dürfen beim Finanzamt vorliegende Daten nicht für andere Ämter genutzt werden? Als Ort nennt Drücker das Bundesamt für Bevölkerungsschutz, das in seiner aktuellen Aufstellung dafür aber nicht ausreicht.

Auch geklärte Zuständigkeit entscheidet noch nicht. Selbst wo entschieden werden darf, fehlt oft die Grundlage: Welche Änderung löst welche Konsequenz aus? Bei Vorhaben mit langen Laufzeiten und vielen Abhängigkeiten wird das zum eigentlichen Zeitfresser – nicht das Abwägen, sondern die fehlende Sicht auf das Gesamtsystem.

conet berät, baut und betreibt. Das Portfolio reicht von der Anforderungsanalyse über Enterprise Architecture Management und Cybersecurity bis zur Softwareentwicklung und zum Betrieb in sicherheitszertifizierten Rechenzentren. Als zweite öffentlich nennbare Referenz führt conet ein mit der Europäischen Verteidigungsagentur entwickeltes Cyber-Lagebild an, entstanden in einem Konsortium mit Fraunhofer, Leonardo und IBM iX.

Erst bauen, dann regeln. Der größte Hebel ist für beide das Machen: eine funktionierende Lösung bauen – die Daten müssen dafür nicht vollständig sein – und erst danach klären, welche Rechtsgrundlage

den verbleibenden weißen Fleck abdeckt. Das wäre zugleich das Signal an den Gesetzgeber. Wie bei der Einführung von KI: erst ein Use Case, Governance und Compliance unterwegs.

REFERENZLÖSUNGEN

Enterprise Architecture Management für Rüstungsprozesse

Gemeinsam mit der BWI bildet conet Rüstungsprozesse in Enterprise-Architekturen ab. Das Vorhaben macht Abhängigkeiten im Gesamtsystem sichtbar und erlaubt es, Bedarfs- und Rüstungsentscheidungen schneller zu bewerten: welche Änderung führt zu welcher Konsequenz.

Der Nutzen liegt vor der Festlegung, nicht danach. Wo heute Folgen erst im Vollzug auftauchen, werden sie zur Entscheidungsgrundlage – in einem Feld, in dem Laufzeiten lang und Korrekturen teuer sind.

Drei Hebel – einfach machen

1. Ressortübergreifend an einem Tisch – pragmatisch, nicht getrieben von der Gesetzgebung.
2. Erst eine funktionierende Lösung bauen, dann Governance und Compliance klären.
3. Haushalt früh absichern: Budget statt Fußnote.

„Es braucht eine übergeordnete Instanz, die die rechtliche Grundlage hat, diese Daten zusammenzuführen – und jemanden, der die Ownership übernimmt.“

Kai Drücker • Chief Commercial Officer • conet

6.4 – WIRKSAMER HANDELN

Wirkung entsteht, wo vorher entschieden wurde



Wirksamer handeln heißt: Kräfte, Mittel und Informationen dorthin bringen, wo sie wirken, und dabei koordiniert bleiben.

Es ist das Feld mit den meisten Praxisbelegen. 55 der 172 erfassten Lösungen zählen darauf ein, 35 sind im Betrieb, acht durch einen dokumentierten Einsatz belegt. Über die dokumentierten Fälle hinweg zeigt sich ein gemeinsames Muster: Wirkung entsteht dort, wo vorher entschieden wurde.

Verbindlichkeit lässt sich vorbereiten. Unter dem Namen Save Berlin hat der Senat gemeinsam mit der Charité die Patientensteuerung per Rechtsverordnung geregelt. Leif Erik Sander beschreibt den Unterschied zur Absprache: Die Zuweisung ist verordnet und wird nicht ausgehandelt.

Freiwilligkeit ebenso. In der Red Farmer Initiative registrieren sich Landwirte in Rheinland-Pfalz, um ihre Fahrzeuge und Geräte der Feuerwehr zur Verfügung zu stellen. Die Steuerung läuft digital in der Einsatzlage. Die Bevölkerung wird so zur nutzbaren Ressource – ohne App und Kampagne.

Auch Vertrauen lässt sich vorbereiten. Schweden unterhält eine Behörde für psychologische Verteidigung. Sie beobachtet Desinformation, veröffentlicht typische Falschmeldungsmuster und bereitet die Bevölkerung auf Manipulationsversuche vor, bevor eine Lage eintritt. Das Fraunhofer FKIE führt dazu militärische Sensorik, Meldungen aus sozialen Netzwerken und die Cyberlage in einem Konzept zusammen.

Nötig ist das, weil Manipulation die Entscheidungsgrundlage selbst angreift. Christian Hummert von der Cyberagentur ordnet Desinformation an die erste Stelle hybrider Angriffe. 20 Einträge aus 16 Interviews behandeln Vertrauenswürdigkeit und Manipulationsschutz. Dem stehen drei Lösungen und eine Maßnahme gegenüber.



„Hybrid wirkt wie eine Schlaftablette. Ich würde es einen Angriff nennen – auf die Gesellschaft, auf die Meinungsbildung.“

Sven Weizenegger • Cyber Innovation Hub, Bundeswehr

Ohne Vorbereitung bleibt auch eine vorhandene Fähigkeit wirkungslos. Für ein ganzes Bundesland stehen zwei Drohnenabwehrzüge bereit. Bis der Zug eintrifft, ist die Drohne weg. Der Betreiber sieht das Objekt über seinem eigenen Gelände und darf nicht handeln. Paul Höller aus dem nordrhein-westfälischen Wirtschaftsministerium schlägt deshalb vor, digitale Abwehr durch die Betreiber selbst rechtlich zu ermöglichen.

Vorbereitung endet nicht bei der Entscheidung, sondern beim Weg zum Einsatzort. CGI liefert mit HERMES verlegbare, verschlüsselte Kommunikation über Satellit, 5G und Zweidraht – die Verbindung steht, bevor die Lage sie erzwingt. MilDef liefert die gehärteten, abstrahl-sicheren Endgeräte, auf denen sie ankommt. Wirksames Handeln setzt einen gemeinsamen Takt von Sensor, Bewertung, Freigabe, Übertragung und Effektor voraus.

CGI

Führungsfähigkeit über Organisationsgrenzen hinweg

CGI IM SICHERHEITSÖKOSYSTEM

Zusammenarbeit beginnt mit kontrollierter Durchlässigkeit

- » Geschlossene Netze über zugelassene Übergänge verbinden
- » Zivil-militärische Schnittstellen tragfähig machen
- » Mobile Führungsfähigkeit bis GEHEIM und NATO SECRET
- » Defence-Praxis aus fast allen NATO-Staaten



Wird Deutschland zur Drehscheibe für die NATO-Ostflanke, sollen binnen eines halben Jahres bis zu 800.000 Kräfte durch das Land verlegt werden – dazu Convoy Support Center, Versorgungsketten, die Rückführung Verwundeter. Zivile und militärische Akteure wollen das gemeinsam bewältigen. Die Frage ist, wie sich die richtigen Informationen sicher verfügbar machen lassen.

Jedes Netz ist für sich geschützt. Bundeswehr, Polizei, Behörden, Landkreise, Energieversorger, Logistikunternehmen und Hilfsorganisationen verfügen über eigene, geschützte IT- und Kommunikationsnetze. Das ist notwendig für ihre Sicherheit – wird aber zur Herausforderung, sobald im Szenario des Operationsplans Deutschland organisationsübergreifende Führungsfähigkeit gefragt ist.

Gesamtverteidigung braucht kontrollierte Durchlässigkeit. Nicht jedes Netz muss mit jedem anderen verbunden und nicht jede Information für jeden verfügbar sein. Entscheidend ist, bestehende Netze über zugelassene Übergänge so zu öffnen, dass jede Organisation genau auf die Lageinformationen zugreift, die sie für ihren Auftrag braucht. CGI schafft diese Übergänge und verbindet bestehende Fähigkeiten, statt ein weiteres isoliertes Netz aufzubauen.

Sicherer Zugang, wo geführt und gehandelt wird. Dafür lassen sich die bereits breit etablierten SINA Workstations nutzen. Wo stationäre Infrastruktur nicht ausreicht, ergänzt CGI sie um mobile, schnell verlegbare Kofferlösungen. So wird hochsichere Kommunikation bis GEHEIM und NATO SECRET auch dort bereitgestellt, wo sie kurzfristig gebraucht wird – unabhängig vom Standort und angepasst an die Einsatzlage.

Technik allein schafft noch keine Führungsfähigkeit. Die Systeme müssen zuverlässig betrieben und die Menschen zu ihrer Nutzung befähigt werden. CGI übernimmt deshalb auch den IT-Betrieb im Hintergrund und unterstützt die Ausbildung. Dabei gilt: so viel Bekanntes wie möglich nutzen, um den Ausbildungsaufwand zu senken.

So entsteht Führung über Organisationsgrenzen hinweg. CGI verbindet bestehende Netze, ermöglicht bedarfsgerechten Zugang zu relevanten Lageinformationen und bringt sichere Kommunikation

dorthin, wo sie gebraucht wird. Damit wird aus einzelnen geschützten Fähigkeiten ein belastbares Zusammenspiel für die Gesamtverteidigung.

REFERENZLÖSUNGEN

HERMES – mobile Führungsfähigkeit der NATO als Blaupause

Das Projekt HERMES ermöglicht der NATO-Kommandostruktur hochsichere mobile Kommunikation bis NATO SECRET – als Koffer transportierbar, über LAN, WLAN, 5G oder Satellit angebunden, mit parallelem Zugriff auf mehrere Sicherheitsdomänen. Auf Basis etablierter SINA-Technologie entstehen binnen weniger Minuten einsatzbereite Führungsarbeitsplätze.

Der Ansatz ist auf die Gesamtverteidigung Deutschlands übertragbar: Im OPLAN-Szenario müssen Bundeswehr, Behörden, Landkreise, zivile Einsatzkräfte, Energieversorger und Logistikunternehmen organisationsübergreifend sicher kommunizieren und handlungsfähig bleiben.

CGI stellt den zuverlässigen Betrieb der auf Technologie von secunet basierenden HERMES-Lösung sicher – mit Service Operation Center, 24/7-Bereitschaft und weltweiter Unterstützung.

Drei Hebel – einfach machen

1. Mit gemeinsamem Mindset anfangen, nicht mit einem Tool.
2. Geschlossene Netze öffnen und Bestehendes verbinden, bevor neue Systeme beschafft werden.
3. Technik einsatzfähig machen – durch Betrieb, Ausbildung und vertraute Lösungen.

„Der kritische Engpass sind für mich klar die geschlossenen Netzwerke. Sie müssen wir aufbrechen, um organisationsübergreifende Zusammenarbeit zu ermöglichen.“

Ansgar Kaltwasser • Vice President • CGI

MILDEF

Kein Führungssystem ohne Gerät

MILDEF IM SICHERHEITSÖKOSYSTEM

Durchhaltefähigkeit beginnt bei der Lieferfähigkeit

- » Robuste Endgeräte in praktisch jedem Gefechtsfahrzeug der Bundeswehr
- » Abstrahlsicherheit serienmäßig statt nachgerüstet
- » Nutzungsdauer fünf bis zehn Jahre statt zwei bis drei
- » Rahmenvertragspartner der Bundeswehr seit 2010



Vor dem Krieg lieferte roda drei- bis fünftausend Geräte im Jahr. In diesem Jahr sind es rund zehntausend, für die kommenden Jahre rechnet Frank Scholz mit zwanzig- bis vierzigtausend. Aus dem Beschaffungsamt kam sinngemäß das Signal: Wer erst anfängt, wenn er den Auftrag hat, ist zu spät.

Durchhalten beginnt beim Gerät. Ein Führungssystem ist nur so verfügbar wie die Hardware, auf der es läuft. Über den Rahmenvertrag der Bundeswehr liefert MilDef – hervorgegangen aus der roda computer GmbH – robuste Endgeräte, Switches, Server, Storage und Peripherie als Träger für Führungs- und Battle-Management-Systeme über alle militärischen Ebenen. Die Geräte stecken heute in praktisch jedem deutschen Gefechtsfahrzeug.

Serienmäßig gehärtet, nicht nachgerüstet. Schock, Vibration, Temperatur, erhöhte elektromagnetische Verträglichkeit – und als Besonderheit eine serienmäßig eingebaute Abstrahlsicherheit, die kompromittierende Emissionen verhindert und in den IT-Konzepten von Bundeswehr und NATO verankert ist. Die Grenze benennt Scholz selbst: Gegen einen nuklearen elektromagnetischen Impuls schützen die Geräte nicht.

Fünf bis zehn Jahre statt zwei bis drei. Kommerzielle Rechner werden nach zwei bis drei Jahren getauscht, diese Geräte laufen fünf bis zehn. Die Basis ist Standard-Hardware, aber in einem Design, das auf Nutzungsdauer statt auf Produktzyklen ausgelegt ist. Durchhaltefähigkeit ist an dieser Stelle vor allem eine Frage der Ersatzteelfähigkeit – und die entscheidet sich Jahre vor dem Ernstfall.

Die Kette hängt an Taiwan. Speicher und Bildschirmpanels kommen ausschließlich von dort; eine europäische Quelle existiert nicht. Speicherpreise haben sich binnen acht Monaten teils verachtfacht, während die Rahmenverträge preisgebunden sind – das Margenrisiko liegt beim Lieferanten. Gemessen am Halbleiter-Rückstand, sagt Scholz, seien die Sondervermögen Taschengeld.

Sechzehn Monate bis zur Zulassung. Der Engpass bei klassifizierten Arbeitsplätzen ist kein Beschaffungs-, sondern ein Qualifizierungsproblem. Hardware ist eng an Software gebunden, weil sicherheits-

relevante Funktionen bis in die Firmware reichen. Allein die CE-Prüfung des Hardware-Designs dauert rund sechzehn Monate, dazu kommen weitere Zertifizierungen und Abstimmungsschleifen.

REFERENZLÖSUNGEN

Rahmenvertrag Bundeswehr seit 2010 – Hardwarebasis im Bestand

Über den Rahmenvertrag liefert MilDef als Katalogware robuste Notebooks, Tablets und Fahrzeugrechner sowie Switches, Server, Storage und Peripherie – Hardwareträger für Führungs- und Battle-Management-Systeme über alle militärischen Ebenen. Hauptkunde ist die Bundeswehr, gefolgt von Systemhäusern wie Rheinmetall, KNDS, Thales und Airbus.

Das Mengengerüst zeigt den Hochlauf: vor dem Krieg drei- bis fünftausend Geräte im Jahr, in diesem Jahr rund zehntausend. Sie stecken heute in praktisch jedem Gefechtsfahrzeug der Bundeswehr. Der eigentliche Durchhalte-Beleg liegt in der Langlebigkeit. Weil Form, Passung und Funktion über Produktgenerationen kompatibel gehalten werden, lassen sich Kettensysteme, die zwanzig bis dreißig Jahre in Nutzung sind, mit Folgeprodukten weiter versorgen. Hinzu kommen gebäudegebundene Lieferungen: In größeren Lagezentren der Bundeswehr stellt MilDef als Unterlieferant sichere Videonetzwerke bereit.

Drei Hebel – einfach machen

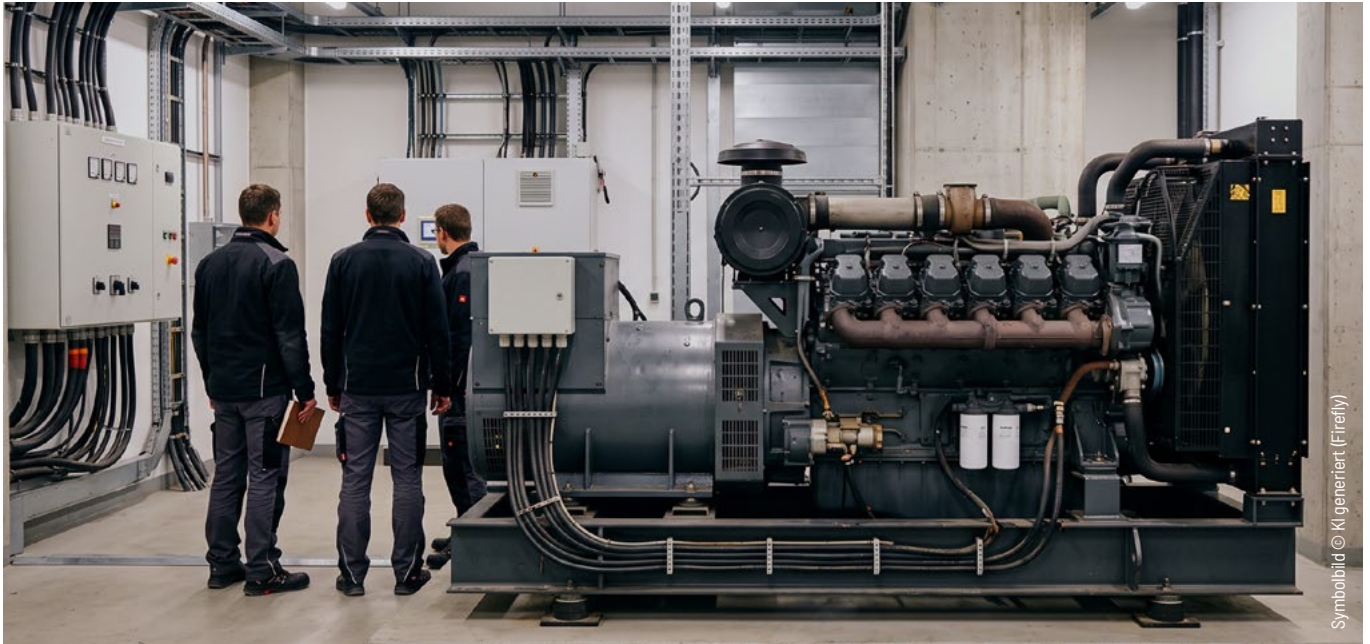
1. Rahmenverträge öffnen – für Behörden mit Sicherheitsauftrag und befreundete Streitkräfte.
2. Beschaffung mit Österreich und den Benelux-Staaten enger zusammenlegen.
3. Meldepflicht zur Gegenseitigkeit machen: Wer meldet, braucht Rückmeldung.

„Im Frieden für den Krieg beschaffen – man muss vom Ziel 2030 rückwärts rechnen, nicht vorwärts.“

Frank Scholz • Geschäftsführer • MilDef

6.5 – LÄNGER DURCHHALTEN

Vorsorge braucht eine verbindliche Vorgabe



Länger durchhalten heißt: den Betrieb sichern, wenn die Störung anhält, und wieder anlaufen, wenn sie vorbei ist.

Durchhaltefähigkeit endet erst, sobald Versorgung, Ersatz oder ein stabiler Betrieb greifen. 41 der 172 erfassten Lösungen zahlen darauf ein, 28 sind im Betrieb, sie zeigen den technischen Beitrag. Die Fähigkeit selbst entsteht aus Technik, Personal, Vorräten, Rückfallverfahren und geübter Priorisierung. Für die Phase nach der Krise finden sich im gesamten Bestand nur zwei Lösungen.

Deutsche Vorsorge entsteht bislang lokal. Der Landkreis Friesland hat Katastrophenschutzleuchttürme eingerichtet, feste Anlaufstellen für die Bevölkerung bei Ausfall von Strom und Kommunikation. Der Kreis Neuwied hat warme Inseln in Dorfgemeinschaftshäusern vorbereitet. Zwei Kreise wählen vergleichbare Lösungen, obwohl eine gemeinsame Vorgabe fehlt.

Wo eine Vorgabe existiert, wird Vorsorge zum Alltag. Südafrika organisiert den Mangel: Bei planmäßigen Lastabschaltungen steuert ein Allokationssystem die rollierende Abschaltung. Eine App zeigt Postleitzahl, Stufe und Abschaltzeitpunkt und erinnert 30 Minuten vorher. Kai Hoberg von der Kühne Logistics University führt dies als Beispiel dafür an, wie Priorisierung im Mangel zum eingeübten Alltag wird. Genau diese Übung fehlt den deutschen Abschaltplänen.

Finnland baut die Vorsorge in die Bausubstanz. Die Baunorm für Schutzräume verlangt, dass Neubauten so errichtet werden, dass sich die Tiefgarage binnen weniger Stunden zum Schutzraum ertüchtigen

lässt – mit Wasser- und Luftversorgung und Betreuungsplätzen. Vier Gesprächspartner aus unterschiedlichen Bereichen haben unabhängig voneinander darauf verwiesen.

Auch die Wirtschaft wird verpflichtet. In Finnland sind ausgewählte Handelsfilialen mit Notstrom ausgestattet und bleiben auch in Krisen versorgungsfähig. Die Schweiz schreibt Unternehmen Lagerreichweiten vor und finanziert sie mit. Hanno Friedrich von der Kühne Logistics University führt beide Modelle an: In beiden Fällen bestimmt der Staat, was vorgehalten werden muss.

Deutschland entwickelt die digitale Vorsorge. Die Bundeswehr baut mit der BWI mobile Rechenzentren – Kapazitäten und Daten, die sich im Krisenfall verlagern lassen. Zwei Wege laufen parallel: eine lokal betriebene Hyperscaler-Variante, ergänzt durch einen eigenen Open-Source-Stack auf kompakter Hardware in Fahrzeugen.

Drei Partner sichern je eine Rückfallebene. AWS verteilt die Rechenleistung über mehrere Verfügbarkeitszonen, weil ein lokales Rechenzentrum allein keinen Sicherheitsgewinn schafft. secunet hält die eingestufte Kommunikation vor – mit SINA als Grundlage und einer für Verschlusssachen zugelassenen Cloud über zwei Rechenzentren. Arvato Systems geht eine Ebene tiefer: eine georedundante Druckstraße, die kritische Daten physisch ausliefert, wenn das Netz weg ist. Was digital nicht mehr trägt, trägt dann Papier.

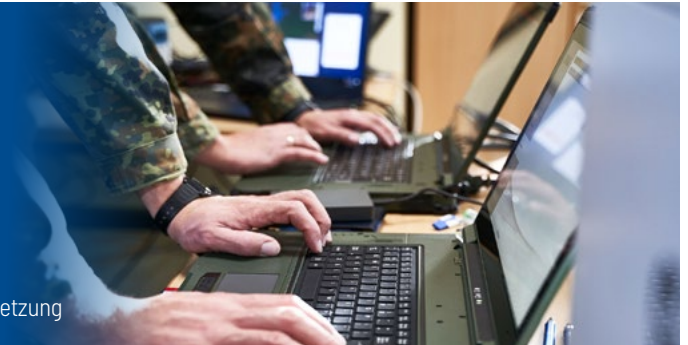
SECUNET SECURITY NETWORKS AG

Sicherheit in der Hinterhand

SECUNET IM SICHERHEITSÖKOSYSTEM

Handlungsfähig bleiben, wenn die eigene Infrastruktur ausfällt

- » Alarmierung, Kommunikation und Kollaboration für Stabteams
- » Im Krisenfall sofort nutzbar, ohne parallele Eigeninfrastruktur
- » In Deutschland gehostet, ISO/IEC 27001, Zugriff über Browser und Authentifizierungsclient
- » Vorbereitete Rollen, Datenräume und Freigabeprozesse als Voraussetzung



Wer wann was in welcher Reihenfolge zu tun hat, ist im Ahrtal theoretisch auf dem Papier geregelt gewesen. Ralph Michel stellt die Frage, die davor liegt: Was geschieht, wenn derjenige, der die Koordination führen soll, im entscheidenden Moment kein funktionierendes Kommunikationsmittel mehr hat?

Es fehlt der vorbereitete Informationsraum. Deutschland hat starke Einzelstrukturen und bewährte Verbünde. Was fehlt, ist der eine zentrale, vorbereitete Raum mit fein zugeteilten Informationen. Vorab zu klären wäre, welche Information bis zu welcher Stufe mit wem geteilt werden darf – damit nicht nur das Operative Führungs-kommando weiß, was zu tun ist, sondern auch Landeskommandos, Kommunen und Energieversorger.

Zero Trust kollidiert mit der Auftragstaktik. Aus Sicht der IT-Sicherheit braucht es minimale Berechtigungen je Rolle. Genau das nimmt dem militärischen Führer das Lagewissen, das die Auftragstaktik zum deutschen Vorteil macht: im Sinne der übergeordneten Führung zu handeln, auch wenn der eigene Auftrag so nicht durchführbar ist. Michel beschreibt das offen als Zielkonflikt, nicht als gelöste Frage.

Kommunen haben kein Budget für Redundanz. Wer seine Wert-schöpfung über digitale Prozesse erbringt, verliert beim Ausfall nicht nur Technik, sondern Handlungsfähigkeit – und öffentliche Träger müssen ihren Auftrag trotzdem erfüllen. Ein zweites, sicheres Kommunikationssystem parallel in Eigenregie zu betreiben, ist auf kommunaler Ebene meist nicht finanzierbar.

Der Beitrag: eine Rückfallebene, die niemand betreiben muss. secunet stellt Stabteams ab 2027 eine Plattform für Alarmierung, Kommunikation und Kollaboration bereit, die sich in getrennte Zugriffsbereiche teilen lässt – etwa für Notfallstab und Krisenstab. Sie ist in der nach ISO/IEC 27001 zertifizierten secunet Cloud in Deutschland gehostet, im Schadensfall innerhalb weniger Minuten einsatz-bereit und braucht zur Nutzung nur einen Browser und einen Authentifizierungsclient. Der Zugriff läuft über ein Authentifizierungs-verfahren, das sich bereits seit Jahren bei der Elektronischen Steuer-erklärung ELSTER bewährt hat.

REFERENZLÖSUNGEN

secunet Notfall- und Krisen-management-Lösung

Wenn die eigene IT ausfällt, fehlt zuerst das, was zur Bewältigung gebraucht wird: ein Kanal, über den der Stab überhaupt noch arbeiten kann. Genau dafür hält secunet ab 2027 eine Plattform bereit, die im Ernstfall nicht erst eingerichtet wird – sie ist schon vorbereitet.

Der Stab meldet, kommuniziert und arbeitet darüber weiter, in getrennten Bereichen für z. B. Notfall- und Krisenstab, und kann weitere Akteure spontan hinzunehmen. Nötig ist dafür nichts als ein Browser und ein Authentifizierungsclient. Betrieben wird die Plattform von secunet, nicht vom Anwender – das ist der Punkt: Kommunen und Behörden bekommen eine Redundanz, für die sie sonst ein zweites System vorhalten müssten.

Was bleibt, ist die Dokumentation: Relevante Aktivitäten werden protokolliert und stehen nach der Lage für die Aufarbeitung bereit.

Drei Hebel – einfach machen

1. Rollen, Datenräume und Freigabeprozesse jetzt festlegen, nicht in der Lage.
2. Unter realistischen Bedingungen üben und das System iterativ nachschärfen.
3. Relevante Daten bis auf die kommunale Ebene schnell bereitstellen – VS-NfD genügt meist.

„Wir brauchen vorbereitete Rollen, wir brauchen Datenräume und Freigabeprozesse – die müssen wir jetzt schaffen. Wenn die Großschadenslage kommt, ist es zu spät.“

Ralph Michel • Global Head of Sales, Division Defence & Space, secunet Security Networks AG

AWS

Digital Backbone, schneller erkennen, entscheiden und handeln

AWS IM SICHERHEITSÖKOSYSTEM

Sicherheit misst sich am Ergebnis – nicht an der Regel

- » Verteilung über mehrere Zonen statt Bindung an einen Standort
- » Rechenleistung vorhalten, nicht im Krisenfall beschaffen
- » Kryptographie nach Schutzniveau statt eines Verfahrens für alles
- » Zulassung laufend validieren statt punktuell alle ein bis drei Jahre



Als die Ukraine angegriffen wurde, zerstörten Angriffe auf Rechenzentren die digitale Infrastruktur in Stunden. Die Regierung verlagerte kritische Systeme binnen Wochen in die Cloud. Die Leitlinie: Handlungsfähigkeit sichern heißt Geschwindigkeit vor Perfektion – Cloud schafft Resilienz und operativen Entscheidungsvorteil durch KI-Analyse, die kein stationäres Rechenzentrum leisten kann.

Ein Rechenzentrum vor Ort ist kein Sicherheitsgewinn. Wo die Anlage steht, entscheidet nicht über Sicherheit – ein einzelner Standort ist ein einzelnes Ziel. Erst die Verteilung über mehrere physisch eigenständige Zonen mit eigener Stromversorgung und Netzanbindung erhält Führungs- und Handlungsfähigkeit, wenn ein Teil ausfällt. AWS betreibt 123 solcher Verfügbarkeitszonen in 39 Regionen; Architekturen darüber erreichen bis zu 99,99 Prozent Verfügbarkeit.

Vom Sensor zur Wirkung in Minuten. Wer schneller erkennt, entscheidet und wirkt, bestimmt das Tempo. Den Kern bildet ein durchgängiges digitales Rückgrat, das die Kette vom Sensor bis zur Wirkung schließt – nicht eine Plattform, die alles können soll, sondern flexibel zusammenwirkende Dienste, über zweihundert davon. Dommels Bild dafür sind Legosteine; als Baukasten für den digitalen Backbone.

Binäre Sicherheitspolitik erzeugt eigene Risiken. Traditionelle Ansätze kennen nur konform oder nicht konform. Eine pauschal vorgeschriebene Typ-A-Kryptographie für alle eingestuft Daten bindet Ressourcen langjährig und schafft Lieferkettenabhängigkeiten; physische Trennung als reine Lehre verhindert die Verbindungen, die im Einsatz nötig sind. Der Ausweg: ein risikobasiertes Modell nach Schutzbedarf.

Isolation alert. Ein abgeschottetes System wird seltener aktualisiert, weil jede Änderung aufwendig und riskant ist. Der Rückstand summiert sich, bis es sich kaum noch ändern lässt, ohne es neu zu bauen. Air-Gap-Netze erzwingen manuelle Transfers, die operative Geschwindigkeit verhindern. Secure by Design setzt dagegen auf laufende, automatisierte Validierung mit maschinenlesbaren Nachweisen – statt Compliance by Checkbox.

Der Beitrag: Befähigung statt Abhängigkeit. AWS versteht die eigene Rolle als Infrastruktur- und Technologieanbieter, der Kunden befähigt, ihre Systeme eigenständig zu betreiben. Das Shared-Responsibility-Modell teilt die Verantwortung: Der Anbieter sichert die Infrastruktur, der Kunde seine Daten und Workloads darin. Mit der European Sovereign Cloud kommt eine ausschließlich in der EU betriebene, von allen anderen Regionen getrennte Infrastruktur hinzu.

REFERENZLÖSUNGEN

Ukraine – Staatsfunktionen unter Beschuss verlagert

Innerhalb der ersten vier Stunden wurden Rechenzentren der ukrainischen Regierung und des Militärs zerstört. Eine Woche vor der Invasion hatte das Parlament die Verlagerung staatlicher Daten in die Cloud erlaubt; die Regierung nutzte diese Grundlage sofort. Binnen 48 Stunden waren erste Daten über mobile Speichergeräte gesichert; am Ende lagen über 15 Petabyte von mehr als 60 Regierungsorganisationen verteilt vor. Darauf setzt der Entscheidungsvorteil auf: Das Gefechtsfeldmanagementsystem Delta integriert Daten von Drohnen, Satelliten und Sensoren zu einem Echtzeit-Lagebild und benötigt dafür über 20.000 Server. KI-gestützte Bildauswertung verkürzte eine zuvor einstündige manuelle Analyse auf wenige Minuten. CSIS stuft Delta als funktionales CJADC2-Äquivalent ein. Der Fall belegt: Cloud-Migration unter Beschuss ist möglich – und Datenhaltung am eigenen Standort wird im Konfliktfall zur Angriffsfläche.

Quellen: AWS Public Sector Blog 2026 · About Amazon 2022 · Nextgov 2022 · CSIS 2025 · AWS-Whitepaper 2026.

Drei Hebel – einfach machen

1. Kryptographie nach Schutzniveau abstimmen statt ein Verfahren für alle Daten.
2. Zulassung laufend validieren statt im Zyklus von ein bis drei Jahren prüfen.
3. Einen Verantwortlichen benennen – und ein Governance-Modell, das Handeln erlaubt.

„Nicht Policy First, sondern Mission First – und Policy Enabled.“

Jens Dommel • Country Manager Public Sector & Defense Germany • AWS

ARVATO SYSTEMS

Auch der digitale Staat braucht einen Plan B

ARVATO SYSTEMS IM SICHERHEITSÖKOSYSTEM

Handlungsfähig, wenn es darauf ankommt

- » Business Continuity Management nach ISO 22301, von der Analyse bis zum Betrieb
- » Georedundanz für kritische Daten – elektronisch und physisch
- » Analoge Rückfallverfahren, wenn digitale Prozesse ausfallen
- » Krisensimulationen und Wiederanlauftests als wiederkehrende Praxis



Bricht die Stromversorgung in einem Einzugsgebiet von 100.000 Menschen zusammen, fallen nicht nur Ampeln, Klärwerke und Heizungen aus. Dr. Norbert Ahrend benennt weitere Folgen für weniger sichtbare Prozesse: Kann eine Verwaltung über vierzehn Tage keine Rechnungen mehr bezahlen, geraten Unternehmen in Liquiditätsprobleme bis hin zur Insolvenz. All das sind Beispiele, die zeigen, warum Resilienz Voraussetzung für staatliche Handlungsfähigkeit ist.

Handlungsfähigkeit gehört nicht in den Keller. Haushalts-, Kassen- und Rechnungswesen-Systeme sind vielerorts nicht so abgesichert, wie es ihre Bedeutung erfordert. Kritische Daten und Anwendungen liegen lokal, bildlich gesprochen „unter der Kellertreppe“, sind nicht georedundant ausgelegt und im Krisenfall nicht erreichbar. Die Handlungsfähigkeit der Verwaltung bleibt auf der Strecke.

Digital ist gut. Resilienz ist Pflicht. Moderne Fachverfahren, digitale Workflows und KI-gestützte Auswertungen machen Verwaltung schneller und leistungsfähiger. Diese Fortschritte sind unverzichtbar – doch sie erhöhen auch das Risiko. Fällt die Infrastruktur aus – durch Cyberangriff, Naturereignis oder Stromausfall –, stehen nicht einzelne Arbeitsschritte still, sondern ganze Prozessketten. Entscheidend ist im Krisenfall nicht, wie Daten erfasst werden, sondern ob sie verfügbar bleiben.

Georedundanz: Verfügbarkeit notfalls auch offline. Kritische Daten und Anwendungen müssen außerhalb des Krisengebiets vorgehalten werden – elektronisch in georedundanten Rechenzentren und, wenn erforderlich, in physischer Form. Erst so gelingt ein geordneter Wiederanlauf. Das Prinzip erinnert an den Cyberangriff „NotPetya“ 2017 auf die Reederei Møller-Maersk: Hier rettete ein isoliertes Backup den Betrieb.

Resilienz für die gesamte Kette. Arvato Systems unterstützt öffentliche Auftraggeber, Digitalisierung von Anfang an belastbar zu machen: Risiko- und Kritikalitätsanalyse, Business Continuity Management nach ISO 22301, Betrieb resilienter Infrastrukturen, Krisensimulationen und Wiederanlauftests, Disaster-Recovery-Konzepte und Cold-/Hot-Standby-Szenarien. Bestenfalls ergänzt durch schwarzfallsichere Kommunikationswege wie die 450-MHz-Infrastruktur.

Üben ist keine Kür. Resilienz entsteht für Dr. Ahrend nicht nur in Konzepten, sondern durch regelmäßiges Üben. Als Vorbild nennt er

das BayZBE in der Oberpfalz, wo organisationsübergreifend Lagertypen trainiert werden – wahrscheinlich der Maßstab, noch nicht die Norm. Aus eigener Erfahrung ergänzt er: Er habe Übungen so real gestaltet, dass die Polizei anrückte.

REFERENZLÖSUNGEN

Digitales physisch absichern

Selbst die modernste digitale Infrastruktur benötigt durchdachte Rückfallverfahren – auch bei vollständigem Netz- und Stromausfall. Schwesterunternehmen von Arvato Systems im Bertelsmann-Konzern betreiben daher georedundant aufgestellte Druckstraßen, die kritische Informationen zyklisch oder bedarfsgerecht drucken und physisch ausliefern können. Damit gehören sie zu den wenigen verbliebenen Anbietern dieser Infrastruktur in Deutschland. Der physische Fallback ergänzt Digitalisierung dort, wo maximale Resilienz erforderlich ist. So stehen die notwendigen Informationen auch dann schon zur Verfügung, wenn noch an der Wiederherstellung und Fortführung digitaler Prozesse gearbeitet wird. Angaben nach Selbstauskunft des Anbieters.

Drei Hebel – einfach machen

1. Festlegen, welche Informationen so kritisch sind, dass sie physisch vorliegen müssen.
2. Zahlungsfähigkeit der Verwaltung georedundant absichern – vor allem die HKR-Systeme.
3. Ebenen- und ressortübergreifend üben, so real, dass es sich echt anfühlt.

„Die Frage ist nicht, ob digitalisiert wird, sondern ob digitale Prozesse auch Krisen überstehen. Im Notfall auch mit analogen Mitteln.“

Dr. Norbert Ahrend • Beratung öffentliche Auftraggeber • Arvato Systems

6.6 – SINNVOLL ORCHESTRIEREN

Orchestrierung ist eine Befugnis, kein Produkt



Sinnvoll orchestrieren heißt, die vier anderen Felder wirksam zu verbinden. Diese Querschnittsaufgabe bildet kein eigenes Feld.

19 der 172 erfassten Lösungen tragen einen Orchestrierungsbezug. Keine davon ist ein Produkt: darunter zehn Konzepte, fünf Programme und ein System. Das ist kein Erhebungsfehler. Es beschreibt, was Orchestrierung ist.

Zwei Länder haben Orchestrierung verfassungsrechtlich verankert.

Finnland fasst unter dem Namen Comprehensive Security umfassende Sicherheit als gesamtstaatliche Aufgabe und führt sie bis auf die Gemeindeebene fort. Schweden weist mit Total Defence jedem Bürger zwischen 14 und 70 eine definierte Rolle im Zivilschutzfall zu. Neun Gesprächspartner dieser Studie haben auf das eine oder das andere verwiesen – die am breitesten belegten Modelle im gesamten Material.

Die Niederlande haben eine Behörde mit dieser Aufgabe betraut.

Rijkswaterstaat verfügt bei Deich- und Wasserfragen über weitreichende Durchgriffsrechte. Sven Ambrosy und Wolfgang Gäbelein nennen es unabhängig voneinander als Modell dafür, wie Orchestrierung praktisch aussieht: als Befugnis.

Deutschland verfügt über ein Zentrum – allerdings nur für ein Thema.

Das Gemeinsame Terrorabwehrzentrum von Bund und Ländern ist die einzige ständige Struktur im Material, in der Sicherheitsbehörden dauerhaft zusammenarbeiten. Tobias Schönherr und Armin Fleischmann führen es als Beleg an, dass es geht. Es entstand nach einem Anlass und bleibt auf diesen Anlass begrenzt.

Ein Bundesland hat eine solche Struktur für die Wirtschaft aufgebaut. Mit defence.NRW verzahnt Nordrhein-Westfalen Landeswirtschaft und Verteidigungsindustrie über Matchmaking, Aufklärung und Beratung. Paul Höller beschreibt es als Cluster, nicht als Behörde – subnational, und im gesamten Bestand ohne Entsprechung.

Technisch liegt genau ein Vorschlag vor: eine Resilienz-API als standardisierter gemeinsamer Andockpunkt, über den alle Systeme an das Lagebild anschließen. Er stammt von Martha Klare und ist ein Vorschlag geblieben.

Vier Partner zeigen, wie Orchestrierung im Kleinen aussieht.

Bechtle arbeitet für sicherheitskritische Infrastrukturen in einem Verbund mit vorab verteilten Rollen – Redundanz, Betrieb, Domänenübergänge und Führungssysteme jeweils aus einem anderen Haus. Sopra Steria deckt äußere und innere Sicherheit in einem Haus ab und setzt an dieser Naht an. soffico beschreibt sie technisch: Baut jedes System eigene Schnittstellen zu vier oder fünf anderen auf, entsteht ein Geflecht, das niemand mehr beherrscht. Eine Zwischenschicht bindet jedes System nur einmal an. msg verfolgt denselben Gedanken für die Lagebilder – verbunden über eine gemeinsame Datengrundlage, die Datenhoheit bleibt beim angeschlossenen System. In allen vier Fällen entsteht die Verbindung aus eigener Initiative.

BECHTLE

Addieren ist nicht integrieren.

BECHTLE IM SICHERHEITSÖKOSYSTEM

Die verbindende Schicht entsteht nicht von selbst.

- » Beide Seiten des Tisches: Beschaffung bei der BWI, heute Systemhaus
- » Vernetzung vorhandener Lagebilder
- » Fähigkeiten beschreiben, statt vorgeben
- » Arbeitsteilung mit Partnern, wo eine einzelne Kompetenz nicht reicht

Bei der Flut im Ahrtal verfügten Militär, Polizei, THW und Feuerwehr jeweils über sehr gute eigene Lagebilder – jede Organisation war für sich handlungsfähig. Was fehlte, war die Vernetzung dieser Lagebilder. Bernd Reitmeier, der in Rheinbach selbst betroffen war, zieht daraus einen Schluss über das System: Die Lücke sitzt nicht in den Fähigkeiten, sondern zwischen ihnen.

Sicherheit erzeugt Inkompatibilität. Den System-of-Systems-Gedanken hält Reitmeier für nicht umgesetzt. Eine Ursache sind besonders sichere Altsysteme, die gerade deshalb nicht koppelbar sind – nicht Nachlässigkeit, sondern Folge der Härtung. Dazu Föderalismus und das Fehlen einer zentralen Verantwortung: Man ist nach Ressorts aufgeteilt, die nicht direkt miteinander kommunizieren.

Zwei Betriebsmodi statt einer Dauerlösung. Wer ein ressortübergreifendes Lagebild orchestrieren sollte, benennt Reitmeier bewusst nicht. Förderierte Datenräume hält er im Normalfall für realistisch; im echten Krisenfall müsse eine Partei befähigt werden, alle Informationen zusammenzubringen. Es brauche jemanden, der entscheidet, wer welche Information benötigt.

Das Vergaberecht ist nicht die Ausrede. Reitmeier kennt beide Seiten: Bei der BWI verantwortete er den strategischen Software-Einkauf, heute steht er auf der Anbieterseite. Bei dringendem Bedarf gelang es dort, im Einklang mit dem Vergaberecht binnen sechs bis zwölf Wochen von der Idee bis zur Lieferung zu beschaffen – möglich nur mit einem Miteinander aller Beteiligten.

Redundanz könnte auf der Schiene liegen. Auf das lettische Data-Embassy-Konzept angesprochen, denkt Reitmeier in eine deutsche Richtung: Container-Rechenzentren, die über das redundante Schienennetz mobil werden – geschickt positioniert oder in stillgelegten Tunneln. Bechtle arbeitet dazu mit der Niedax-Gruppe und deren Projekt Netz33, das entlang der Bahntrassen ein eigenes Netz aufbaut. Die Vorhaben stehen am Anfang; die schnelle Datenmigration bleibt ungelöst.

Fähigkeiten beschreiben, nicht Lösungen vorgeben. Der größte Hebel ist für Reitmeier die Entscheidung selbst: Verantwortung übergeben, Fähigkeiten aufbauen, den Betrieb delegieren – eine

Behörde beschreibt, was sie können muss, statt vorzugeben, womit. Das entspricht dem Geschäftsmodell eines Systemhauses: aus Fähigkeitsanforderungen Lösungen zu bauen.

REFERENZLÖSUNGEN

Das Partnernetzwerk – Orchestrierung im Kleinen

Für sicherheitskritische Infrastruktur arbeitet Bechtle in einem Verbund mit vorab verteilten Rollen: Netz33 schafft die physische und logische Redundanz, Bechtle integriert und betreibt die IT-Komponenten, infodas liefert die Übergänge zwischen Sicherheitsdomänen, Systematic die militärischen Führungs- und Informationssysteme.

Der Punkt ist nicht die Liste der Beteiligten, sondern die Reihenfolge: Abgestimmt wird in der Konzeptionsphase, nicht bei der Integration. Reitmeiers eigener Satz dazu – die größten Effekte entstehen dort, wo Kompetenzen nicht addiert, sondern integriert werden.

Als Anwendungsfelder nennt der Verbund unter anderem den Territorial Hub und das Krisenvorsorgeinformationssystem des Bundes.

Drei Hebel – einfach machen

1. Mit dem operativ Bewährten beginnen, statt auf die allumfassende Lösung zu warten.
2. Den Stressfall üben – nicht nur Einzelsysteme in sicherer Umgebung erproben.
3. Für den Krisenfall vorab festlegen, welche Partei alle Informationen zusammenführen darf.

„Entscheidungen treffen.“

Bernd Reitmeier • Leitung Account Management BWI • Bechtle

SOPRA STERIA

Dreißig Sekunden, vier Zuständigkeiten – Handlungssicherheit schaffen

SOPRA STERIA IM SICHERHEITSÖKOSYSTEM

Multi-Domain-Defence gegen hybride Bedrohungen durch Drohnen und Cyberangriffe

- » Zusammenarbeitsmodell für die Drohnen- und Cyberabwehr
- » Klare Zuständigkeiten im Föderalismus
- » Innere und äußere Sicherheit integriert gedacht
- » Schnell verlegefähige Abwehrsysteme in die Gesamtlage integrieren



Fliegt eine Drohne zwischen Bundeswehrliegenschaft, Autobahn, Bahnstrecke und Raffinerie hin und her, berührt sie in wenigen Minuten und teils nur Sekunden drei bis vier Zuständigkeitsbereiche. In der Verdichtung der Geografie wird erkennbar, dass sich das Bedrohungspotenzial schnell um ein Vielfaches multiplizieren kann. Flankierende Cyberangriffe potenzieren die Risiken. Konvergierende Bedrohungen verlangen ein Cyber-Physisches Verteidigungszentrum.

Der Rechtsrahmen hinkt der Bedrohung hinterher. KRITIS-Betreiber dürfen im Nahbereich ihrer Anlagen derzeit nicht selbst im Luftraum wirken; Sicherheitsbehörden können keinen flächendeckenden Schutz aller KRITIS gewährleisten. Die Kernfrage ist daher nicht die Technologie, sondern der Rechtsrahmen: Wie schaffen Bund und Länder ein rechtssicheres, anpassungsfähiges Regelwerk für die Abwehr hybrider Bedrohungen durch Sicherheitsbehörden, Militär, KRITIS-Betreiber sowie Sicherheits- und IT-Dienstleister? Konkret: Wer darf mit welchen Mitteln unter welchen Bedingungen im Cyber- und physischen Raum handeln?

Ein zweistufiges Modell der Zusammenarbeit. Erforderlich ist ein sektorspezifisches Empowerment der KRITIS-Betreiber. Stufe 1: Betreiber bzw. Dienstleister detektieren, klassifizieren, bewerten und im Rahmen ihrer Befugnisse neutralisieren physische und Cyberbedrohungen anhand definierter Kriterien. Stufe 2: Eskalation an eine behördliche Zentrale mit erweiterten Rechten und Mitteln zur Remote-Neutralisierung. Grundlage ist ein gemeinsames cyber-physisches Lagebild für Betreiber, Behörde und Dienstleister. Die staatliche Hoheit bleibt gewahrt. Offene Punkte sind Qualifikation, Zertifizierung und Befugnisgrenzen der Akteure. Erst daraus entstehen Handlungssicherheit und tragfähige Geschäftsmodelle.

Beitrag von Sopra Steria zu Multi-Domain Defence. Der europäische Digitalisierungs- und IT-Sicherheitsdienstleister deckt äußere und innere Sicherheit in einem Haus ab: Als führender europäischer Partner im Bereich der digitalen Souveränität mit starkem Beitrag zum Aufbau der strategischen Autonomie Europas. An dieser Naht setzt der Fähigkeitsbeitrag an. Mit BOREADES bringt Sopra Steria ein Command-and-Control-System für die Drohnenabwehr ein: full Counter-UAS Kill-Chain mit Multisensor-Datenfusion im Kern, agnostisch gegenüber Sensoren und Effektoren, ITAR-free und anschlussfähig und interoperabel mit der integrierten Luftraumüberwachung.

Auf der Cyberseite stellt Sopra Steria mit dem NextGen SOC eine KI-gestützte Plattform bereit, die Cyberbedrohungen in Echtzeit erkennt, priorisiert und abwehrt und durch Automatisierung sowie 24/7-Betrieb die Reaktionsfähigkeit deutlich erhöht. Mit CENTERIS von Sopra Steria ist die integrierte Sicherheits- und Resilienzplattform zur Erkennung, Bewertung und Abwehr konvergierender Bedrohungen aus Cyberraum und physischer Welt verfügbar.

REFERENZLÖSUNGEN

Paris 2024 – Olympische Spiele gesichert

Bei den Olympischen und Paralympischen Spielen Paris 2024 bewährte sich BOREADES als technologische Basis einer umfassenden Counter-UAS-Sicherheitsarchitektur. CS GROUP, ein Unternehmen der Sopra Steria Gruppe, stellte gemeinsam mit ihren Partnern insgesamt 14 Systeme zur Drohnerdetektion und -neutralisierung bereit und unterstützte die Sicherheitsbehörden bei Training, Implementierung, Deployment und operativem Betrieb. Die modularen Systeme wurden an unterschiedlichen Standorten in Paris und Marseille eingesetzt und in die zentrale Drohnenabwehrarchitektur der französischen Luftstreitkräfte integriert.

Drei Hebel – einfach machen

1. Betreiber ermächtigen – je nach Anlagentyp, nicht pauschal.
2. Kriterien für Drohnenabwehr-Dienstleister festlegen.
3. Iterativ in schnellen kleinen Schritten vorgehen, nicht im Big Bang.

„Europa braucht Akteure, die Sicherheitsfähigkeiten über Behörden-, Branchen- und Domänengrenzen hinweg verbinden.“

Axel Lips • Head of Client Unit Defence Germany, Sopra Steria

SOFFICO

Systeme verbinden statt Spaghetti-Interfaces vervielfachen

SOFFICO IM SICHERHEITSÖKOSYSTEM

Die Systeme sind da. Die Zwischenschicht fehlt.

- » Systeme einmal anbinden – herstellernerneutral und wiederverwendbar
- » Connector-Prinzip aus der Industrie, heterogene Daten und Systeme semantisch verbinden – von Edge bis Core
- » Informationsflusskontrolle: Datenflüsse sicher steuern – auch über Klassifizierungsgrenzen hinweg
- » Souverän entwickelt in Deutschland – für vernetzte zivil-militärische Architekturen



In Land, Luft und See existieren zahlreiche Lage- und Battle-Management-Systeme, die miteinander kommunizieren könnten – aber nicht uneingeschränkt. Bei der Landesverteidigung kommen Polizeien, Katastrophenschutz und Feuerwehr hinzu, jede mit eigenen Systemen. Für Bernd Hellinger gehört selbst das Informationssystem der Autobahngesellschaft dazu, weil es im Verteidigungsfall zählt.

Kein Technikproblem, ein Verbindungsproblem. Die Systeme seien vorhanden und in aller Regel gut, sagt Hellinger – die Herausforderung liege in ihrer Vielzahl und darin, dass ein einfacher, systemübergreifender Datenaustausch häufig nicht unterstützt wird. Baut jedes System eigene Schnittstellen zu vier oder fünf anderen auf, entsteht ein Geflecht, das niemand mehr beherrscht. Im Haus soffico heißt das seit Jahren das Spaghetti-Interface.

Vor dem großen Lagebild steht das Verknüpfen der einzelnen. Das militärische Lagebild wird heute nicht umfassend mit dem zivilen angereichert; es fehlt die Integration, die aus vielen Lagebildern eines macht. Der Weg dorthin führt nicht über den großen Wurf: Erst wenn die einzelnen Bilder verknüpft sind, kann für eine konkrete Lage ein umfassendes, bedarfsgerechtes Bild bereitstehen.

Einmal bauen, überall wiederverwenden. Das Prinzip stammt aus der Fertigung: Ein Unternehmen koppelt sein ERP-System (IT) nicht einzeln an jede Maschinensteuerung (OT), sondern über eine Middleware mit wiederverwendbaren Connectoren. Auf die Verteidigung übertragen heißt das, jedes System nur einmal anzubinden. Am volatilen Drohnenmarkt wird die Dringlichkeit sichtbar: Man kann nicht jeden Hersteller einzeln anschließen, sondern braucht einen „Stecker“, der mehrere Systeme zugleich erreicht.

Der Zugang zu den Standards ist das Nadelöhr. Ein Hersteller mit innovativer Schwarmsteuerung muss seine Daten in militärische Standards überführen, um sie in Lagebildsysteme einzuspeisen. Weil die Spezifikationen klassifiziert sind und ohne bestehenden Auftrag nicht bereitgestellt werden, bremst das genau jene aus, die Konnektivität herstellen könnten.

Der Beitrag: nur Konnektivität, bewusst fokussiert. Orchestra Defence Service Bus ist eine herstelleragnostische Low-Code-Integrationsplatt-

form, die Systeme mit unterschiedlicher Datensemantik verbindet, ohne die Anbindung jedes Mal neu zu bauen. Hinzu kommt eine Informationsflusskontrolle, die verhindert, dass eingestufte Daten in ein niedriger klassifiziertes System abfließen – und zugleich erlaubt, Informationen von unten gezielt ins militärische Lagebild hochzuführen.

REFERENZLÖSUNGEN

Drohenschwarm-Steuerung – Anbindung an die Systemwelt

In einem laufenden Projekt arbeitet soffico mit einem Hersteller von Software zur Steuerung von Drohenschwärmen zusammen. Dessen System übernimmt die Missionsplanung – welche Drohnen mit welchen Sensoren zum Einsatz kommen – und die Minimal-kommunikation während der Operation.

soffico nimmt die entstehenden Daten auf und überführt sie in die geltenden militärischen Standards, damit sie in Lagebild- und Battle-Management-Systeme einfließen. Nach dem Einsatz folgt der oft unterschätzte Teil: Batteriemanagement, Motordaten, Logdateien und Videosequenzen werden über die Funkstrecke nicht vollständig übertragen. Sie werden eingesammelt, aufbereitet und normgerecht in die Bibliotheken der Lagebildsysteme überführt.

Der Kerngedanke: Ein hochspezialisierter Innovator bleibt bei seiner Technik, die Zwischenschicht übernimmt die Anbindung.

Drei Hebel – einfach machen

1. Zugang zu militärischen Standards öffnen, bevor ein Auftrag vorliegt.
2. Mehrere Anbieter parallel mit Prototypenbudget beauftragen.
3. Die operative Ebene ermächtigen, statt Innovation von oben zu steuern.

„Bevor ich zum großen Lagebild komme, muss ich erst die einzelnen verknüpfen.“

Bernd Hellinger • Verteidigung & Sicherheit • soffico

msg

Zwei Lagebilder, kein Übergang

msg IM SICHERHEITSÖKOSYSTEM

Gemeinsame Semantik statt zentraler Plattform

- » Dezentrale Lagebilder auf gemeinsamer Datengrundlage
- » Datenhoheit bleibt beim angeschlossenen System
- » Übersetzung zwischen DV 102 und militärischen taktischen Zeichen
- » Offene Schnittstellen, ohne Anspruch auf Exklusivität



Bringt die Bundeswehr bei einer Übung ihre Lagebildsysteme in ein gemeinsames Lagezentrum mit, steht daneben ein Verbindungsoffizier und überträgt von Hand. Auf der zivilen Seite ist das Lagebild manchmal gar keine Software, sondern ein Magnetbrett. Felix Wang diente dreizehn Jahre in der Bundeswehr, ist aktiver Reservist und arbeitet heute an IT-Lösungen für den Verteidigungssektor.

Die Naht ist die Struktur — und der Feind zielt darauf. Föderale Ordnung und Ressortlogik trennen, was im Ernstfall zusammenwirken müsste; im zivilen Bereich setzt sich die Trennung über Länder und Gemeinden fort. Wo Zuständigkeiten aneinanderstoßen und niemand genau weiß, was der andere gerade tut, entsteht die verwundbarste Stelle des Systems — und ein Angreifer wird sie nutzen. Eine Umweltkatastrophe hält sich nicht an Landesgrenzen, ein Feind erst recht nicht.

Der Verbindungsoffizier kommt nicht mehr hinterher. Die menschliche Schnittstelle ist der Bruch. In einer hochdynamischen Lage reicht sie nicht: Bevor die Übersetzung fertig ist, hat sich die Lage bereits verändert. Was es braucht, ist Interoperabilität zwischen Maschinen — nicht zwischen Menschen, die zwischen Systemen vermitteln.

Nicht eine Lage, sondern viele. Weil Feuerwehr, Polizei, THW und Bundeswehr verschiedene Aufträge haben, brauche es viele Lagebilder auf identischer Datengrundlage, aber mit unterschiedlichen Sichten. Die Aufgabe liegt in der Übersetzung. Militärische taktische Zeichen und die zivile Dienstvorschrift 102 lassen sich nicht eins zu eins überführen, weil dahinter unterschiedlicher Informationsbedarf steht.

Die offene Frage lautet: Wer ist für die Vernetzung zuständig? Beim Fortschritt bleibt Wang nüchtern: Seit dem russischen Angriffskrieg habe sich viel bewegt, im Bild des Fortschrittsbalkens stehe man dennoch bei dreißig bis vierzig Prozent. In einem Land, das gern klärt, wer für was zuständig ist, fehlt ausgerechnet die Antwort darauf, wer für die Vernetzung zuständig ist. Das größte Eigeninteresse habe die Bundeswehr — doch wo militärische Logik auf Länder und Gemeinden trifft, kann sie nur koordinieren.

Der Beitrag: orchestrieren, ohne zu zentralisieren. msg.Relais ist eine Data-Streaming-Lösung, die Lagebildsysteme orchestriert, ohne die Datenhoheit zu zentralisieren — die Daten bleiben in dem System,

das angeschlossen wird. Kern ist eine Transformation Engine, die Standards verknüpft und Übersetzungen KI-gestützt vorschlägt; die abschließende Entscheidung bleibt bei der Organisation. Das Haus dahinter ist eine Aktiengesellschaft in vollständiger deutscher Eigentümerhand; siebzig Prozent der Mitarbeitenden im Geschäftsbereich Defense and Aerospace sind ehemalige Soldaten.

REFERENZLÖSUNGEN

Lagebildvernetzung in Erprobung

Im Testlabor von msg sind drei Systeme (LAGEskizze, CivTAK und Sitaware) verbunden. Ziel ist der Anschluss an das Lagebild der Bundeswehr, wofür das Vorhaben TerrHubBw die interessanteste Variante darstellt.

Den Anstoß gab eine Studie zum ressortübergreifenden Lagebild: Während militärisch viel vorangetrieben wurde, klafft auf der zivilen Ebene — bei Behörden mit Sicherheitsaufgaben und KRITIS-Betreibern — noch eine große Lücke.

Ein dritter Platz bei der Innovationstagung des BMVg 2026 hat Folgegespräche eröffnet; erste Kontakte zu Katastrophenschutz und integrierten Leitstellen bestehen.

Drei Hebel — einfach machen

1. Bestände vernetzen statt Monolithen beschaffen.
2. Offene Interoperabilitätsstandards zwingend vorschreiben.
3. Datenhoheit durch granulare Föderation garantieren statt Daten zentralisieren.

„Der Schlüssel liegt nicht im Ersetzen gewachsener Systeme, sondern in deren automatisierter Übersetzung. So bleibt jeder Akteur in seiner bedarfsgerechten Umgebung.“

Felix Wang • Defense & Aerospace • msg

6.7 – DER AUFTRAG

Was die Beschaffung jetzt anders machen muss

Damit aus einzelnen Elementen ein Rückgrat wird, muss der Markt sechs Voraussetzungen schaffen. Keine verlangt ein neues Produkt, entscheidend sind die Bedingungen der Entwicklung und Beschaffung.

Offene Schnittstellen als Vergabebedingung. Sie müssen als Ausschlusskriterium gelten. Eine Empfehlung oder unverbindliche Zielarchitektur reicht nicht. 25 der 41 Anbieter aus der Befragung geben an, standardisierte und dokumentierte Schnittstellen bereitzustellen. Die Fähigkeit ist da. Es fehlt die verbindliche Nachfrage.

Ein Angebot für die Zeit danach. Von 172 erfassten Lösungen adressieren zwei den Wiederanlauf. Vorsorge lässt sich ausschreiben, für die akute Lage wird Budget mobilisiert. Der Wiederanlauf beginnt nach dem Ende der öffentlichen Aufmerksamkeit. Solange niemand danach fragt, entsteht dort nichts.

Preise, die man vergleichen kann. Weder in den dreizehn Partnerbeiträgen noch im übrigen Bestand nennt ein Anbieter ein Kostenmodell. Wer die Kosten nicht kennt, kann kaum priorisieren. Gerade im Mangel ist Priorisierung eine Kernaufgabe.

Angebote, die eine Kommune erreichen. Unter den Referenzprojekten der dreizehn Partner findet sich keine einzige kommunale Lösung. Auch in der Befragung schneiden rein kommunale Lösungen deutlich schwächer ab als Lösungen für Bund und internationale Ebene. Der Zwischenwert fällt auf: Die höchste Reife zeigt sich bei gemeinsamer Adressierung von Kommune und Land. Eine übergeordnete Ebene trägt damit zur Umsetzungsreife bei, obwohl die Lagen vor Ort beginnen.

Eine Antwort auf die Haftungsfrage. Wer steht ein, wenn eine gekoppelte Lösung im Ernstfall ausfällt? In keinem der Gespräche wird sie erwähnt. Solange die Frage offenbleibt, koppelt niemand freiwillig über die eigene Systemgrenze hinaus – und wer es doch tut, tut es auf eigenes Risiko. Für Hilfsorganisationen und gemeinnützige Träger, die aus Spenden und Fördermitteln arbeiten, ist das eine Existenzfrage.

Eine fortlaufende Marktübersicht. Ein solches Verzeichnis müsste dauerhaft den gesamten Markt erfassen: nach Wirkung geordnet, mit ausgewiesenem Belegstatus und sichtbaren Leerstellen. Momentaufnahmen veralten. Eine gepflegte Übersicht macht Lücken im Zeitverlauf sichtbar und schafft eine Grundlage für die Beschaffung. Wer sie führt, bleibt offen: ein Bundesamt, eine Beschaffungsorganisation, ein Verband.

Beschaffung, Gesetzgeber und Anbieter sind gefordert. Die Beschaffung bestimmt Schnittstellen, Preise und die Reichweite kommunaler Angebote – sie ist der Hebel für vier der sechs Punkte. Der Gesetzgeber klärt die Haftung. Die Anbieter müssen die Kopplungsschicht bereits vor einer Bestellung als Geschäftsfeld entwickeln.

Das folgende Kapitel ordnet die Schritte nach Reihenfolge und Termin.

07

Von der Vision zur Umsetzung

Wie Deutschland handlungsfähiger wird

7.0 – DIE HANDLUNGSFELDER

Dreißig Maßnahmen, jede mit Träger und Frist



Eine Maßnahme beginnt bei einem Träger, einer Frist und einem überprüfbaren Nachweis.

Aus 529 Vorschlägen in 55 Interviews verdichtet das vorliegende Kapitel 30 Maßnahmen in sechs Handlungsfeldern und verbindet sie mit dem Innovationsraum und einer Zielmarke für 2030.

Neue Technologien verändern Krisen schneller, als klassische Beschaffung sie in die Fläche bringt. Sensorfusion, Künstliche Intelligenz, autonome Systeme, Weltraumtechnik und Dual-Use-Ökosysteme zeigen, wie sich Entscheidungszeit und Handlungsmöglichkeiten verschieben. Erprobung und flächige Fähigkeit sind dabei zweierlei. → [7.1](#)

Das gemeinsame Lagebild ist der meistgenannte Mangel der Studie. Vorhandene Netze, Sensoren und Systeme sollen über definierte Übergänge verbunden werden. Ein förderierter Datenraum schafft den Rückkanal zu Ländern und Betreibern. Der Weg führt vom vorhandenen Bestand zum zivil-militärischen Lagebild. → [7.2](#)

Governance lässt sich an vielen Stellen unterhalb einer großen Strukturreform verbessern. Übergangsschwellen, regelmäßiger Austausch, frühe Anwendungsfälle, Vollzeitkräfte und verteilte Pflichten verlagern Entscheidungen aus der akuten Lage in die Vorbereitung. Führung besteht damit aus einer Reihe überprüfbarer Vor-entscheidungen. → [7.3](#)

Ressourcen entscheiden über Tempo und Durchhaltefähigkeit: Rahmenverträge, Verbrauchsgüter, Meldekanäle, Transitwege, Cloud-Architekturen und Forschungssicherheit. Der Engpass reicht vom Beschaffungsrecht bis zur Frage, welche Brücke einen militärischen Transport trägt. Auch Ressourcen brauchen Träger, Frist und Nachweis. → [7.4](#)

Schutz und Abwehr treffen auf Angriffe, die physische und digitale Mittel kombinieren. Lagebilder, gehärtete Kliniken, Drohnenabwehr und ein handlungsfähiger Cyber-Krisenstab müssen deshalb entlang einer gemeinsamen Reaktionskette gedacht werden. Erkennen, Entscheiden und Wirken gehören in einem Schutzfeld zusammen. → [7.5](#)

Resilienz entscheidet vor, während und nach dem Treffer. Betankung, Wiederanlauf, zivil-militärische Verträge sowie die Abwehr chemischer, biologischer, radiologischer und nuklearer Gefahren brauchen vorbereitete Ketten. Eigenvorsorge der Bevölkerung erweitert die verfügbare Zeit in den ersten 72 Stunden. Der größte Maßnahmenblock richtet sich auf Durchhalten und Wiederanlauf. → [7.6](#)

Gesellschaftliche Handlungsfähigkeit beginnt bei Menschen, die ihre Rolle kennen. Bevölkerung, Ehrenamt, Verwaltung und politische Entscheidungsträger brauchen Übung, Ausbildung, Anlaufstellen und klare Kommunikation. Freiwillige Hilfe wird damit von einer spontanen Kraft zu einer planbaren Ressource. → [7.7](#)

Die 30 Maßnahmen sind als Quick Wins, also schnell startbare Schritte, und Bold Moves, also politisch anspruchsvolle Entscheidungen, geordnet. Jedes Handlungsfeld schließt mit einem New Horizon – einer Aufgabe, die über den Zeithorizont der Maßnahmen hinausreicht und deshalb nicht mitzählt. Träger, Fristen und Nachweise sind Vorschläge dieser Studie. Die Fristen laufen ab der verbindlichen Beauftragung. Ihre gemeinsame Grenze ist eine politische Zielmarke – und damit die Frage: Wie gut wollen wir sein? → [7.8](#)

7.1 – DER INNOVATIONSRAUM

Für die nächste Krise rüsten, nicht für die letzte

Sensorfusion, Künstliche Intelligenz, autonome Systeme und Weltraumtechnik verschieben den Charakter einer Krise. Ihr Weg vom Prototyp in die Fläche offenbart den deutschen Engpass. Der Cyber Innovation Hub der Bundeswehr bearbeitet rund 40 Projekte im Jahr, ein Teil davon mit Bezug zu Krisen und Lagen, daneben entstehen Innovationen an vielen weiteren Stellen des Ökosystems.

Sensorik erzeugt das Lagebild, bevor die Lage eintritt. Ein Vorhaben zur Multi-Sensor-Datenfusion führt Daten vom Meeresboden bis in den Weltraum zu einem einheitlichen Bild zusammen und ist in Rostock im Einsatz. Man dürfe das Lagebild nicht erst zusammenschustern, wenn der Fall eingetreten sei, sagt Sven Weizenegger vom Cyber Innovation Hub der Bundeswehr – dann sei es zu spät. Sieben Lösungen im erfassten Bestand gehören zu diesem Feld.

Künstliche Intelligenz verschiebt die Dimension Zeit. Ein von Menschen erstelltes Lagebild ist entweder schnell verfügbar oder genau. Christian Marwitz von der BWI sieht darin den entscheidenden Effekt und formuliert die Kette: Informationsüberlegenheit führt zu Führungsüberlegenheit führt zu Wirkungsüberlegenheit. Marianne Janik von Google Cloud beschreibt, was heute schon einsetzbar wäre: Tausende Agenten arbeiten parallel an unterschiedlichen Hypothesen und liefern eine priorisierte Lagebeurteilung. Entscheidend seien klare, hochspezialisierte Rollen, statt einen Agenten alles erledigen zu lassen. Das Feld umfasst 21 Lösungen, keine weist einen Praxisbeleg auf.

Autonome Systeme senken die Kosten der Abwehr. Ein Interceptor-Prototyp aus München soll Aufwand und Kosten beim Abfangen gegnerischer Drohnen deutlich senken. In der elektronischen Kampf-

führung denkt der Hub Systeme als Wegwerfartikel: kleine Emitter, per Hand, Drohne oder Artillerie ausbringbar, vermascht und bewusst günstig – bei Verlust einzelner Knoten degradiert die Leistung, statt auszufallen. Mit fünf Lösungen ist dieses Feld von allen acht am dünnsten besetzt.

Der Weltraum fällt zuerst aus. Auf die Frage nach dem ersten Ausfall im Bündnisfall nennt Benedikt Meng von infodas die Satellitenkommunikation: Cyberoperationen gegen Kommunikationsnetze, gestörte Verbindungen, GPS-Spoofing – die Zugänge dafür seien vermutlich längst gelegt. Führung und Aufklärung lägen zu großen Teilen im Orbit, der Engpass seien die europäischen Startkapazitäten. Das Feld umfasst 14 Lösungen, zwei davon mit Praxisbeleg.

Was davon in die Fläche kommt, ist die eigentliche Frage. Ein einsatztaugliches Minimalprodukt sei rasch gebaut, sagt Weizenegger, bis es die Truppe in der Fläche erreiche, vergingen Jahre. Das System denke nur in großer Skalierung, nicht in einer ersten Befähigung. Von 131 Interview-Nennungen tragen 16 einen Praxisbeleg. Die Zuordnung zu den acht Innovationsfeldern ist handcodiert und keine Marktgröße. Aussagen über Reife und Marktangebot stützen sich auf die 41 Anbieter-Selbstausskünfte der Online-Befragung.

EBENE 7 · INNOVATION

In jedem Feld läuft etwas. Erprobt fast nirgends.

11 ●●● Krisenführung Das Lagebild entsteht laufend, nicht auf Anforderung. Fusion aus Bürger, Polizist und Drohne in Echtzeit, Ukraine Airbus Defence and Space	12 ●○○ Cyber & Infosicherheit Der Angriff kommt digital und physisch zugleich. Angriff auf Steuerzentralen plus Sabotage kippt das Netz Google Cloud	13 ●●○ KI & Datenanalyse Vorwarnzeit entsteht aus Rechenleistung, nicht aus Personal. Agentische Lagebeurteilung: tausende Agenten prüfen Hypothesen parallel Google Cloud	14 ●○○ Autonome Systeme Die Handlung beginnt, bevor jemand entscheidet. Interceptor-Prototyp senkt die Kosten der Drohnenabwehr Cyber Innovation Hub
15 ●●○ Weltraum & Satellit Führung liegt im Orbit – und fällt dort zuerst aus. Erster Ausfall im Bündnisfall: Satellitenverbindung, GPS-Spoofing INFODAS	16 ●●● Energie & Logistik Durchhaltefähigkeit wird verlegbar statt gelagert. Netzleitstelle doppelt geführt, Satellitentelefon, zweiter Standort Energienetzbetreiber	17 ●○○ Sensorik & Aufklärung Das Lagebild trifft vor den Einsatzkräften ein. Multi-Sensor-Fusion vom Meeresboden bis in den Orbit, im Einsatz in Rostock Cyber Innovation Hub	18 ●●○ Dual-Use-Ökosysteme Fähigkeit entsteht schneller, als sie beschafft wird. 14 laufende Projekte, Gehirn-Computer-Schnittstelle weltweit auf Platz 2 Cyberagentur

Abb. 7.1: Zielbild GSÖ 2030, Ebene 7

7.2 – DAS LAGEBILD

Lagebilder vernetzen statt eins für alle bauen

Im Handlungsfeld Information und digitales Rückgrat entstehen Lagebilder, Systeme werden verknüpft und Kommunikationswege bleiben bestehen, wenn andere ausfallen. Mit 129 Vorschlägen ist es das breitest getragene Feld der Studie.

Fünf Maßnahmen greifen ineinander. Drei Quick Wins nutzen Vorhandenes: Sie machen die beiden bekannten Übergänge frei, binden bestehende Bestände an und verdichten die Netze. Zwei Bold Moves bauen darauf auf – der föderierte Datenraum, der die Einspeisung belohnt, und das zivil-militärische Lagebild, das daraus eine Entscheidungsgrundlage macht. Keine davon verlangt ein neues System.

QUICK WIN Die zwei bekannten Übergänge deblockieren

Zwei benannte Schnittstellen zwischen militärischer und ziviler Seite existieren und funktionieren nicht. Die Schwarz-Rot-Gateways führen zwischen eingestuft und offenen Netzen, standardisiert ist bisher nur eine Richtung. Armin Fleischmann warnt davor, die zivile Seite zu überschätzen: „Glauben Sie nicht, dass die offene Seite so weit ist wie wir.“ Die Funkbrücke zur Bundesanstalt für den Digitalfunk der BOS hängt an industriepolitischen Fragen.

Träger und Nachweis: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die BWI standardisieren die Spezifikation, die zivilen Ressorts rüsten die offene Seite nach. Nach zwölf Monaten läuft eine Referenzimplementierung zwischen Bundeswehr und einem zivilen Ressort.

QUICK WIN Vorhandene Bestände anbinden statt neu bauen

Sensorik und Ressourcen, die längst existieren, lassen sich zweckgebunden einbinden, ohne dass etwas beschafft wird. Norbert Ahrend nennt zwei Beispiele: Die Berliner Verkehrsbetriebe betreiben ein Kamerasystem, das im Krisenfall Lagebilder liefern könnte, und in Rheinland-Pfalz registrieren Landwirte über die Red Farmer Initiative freiwillig ihre Maschinen für die Feuerwehr.

Träger und Nachweis: Die Betreiber selbst, abgesichert über Zweckbindungsvereinbarungen mit der Katastrophenschutzbehörde. Nach zwölf Monaten bestehen zwei solcher Vereinbarungen in unterschiedlichen Sektoren.

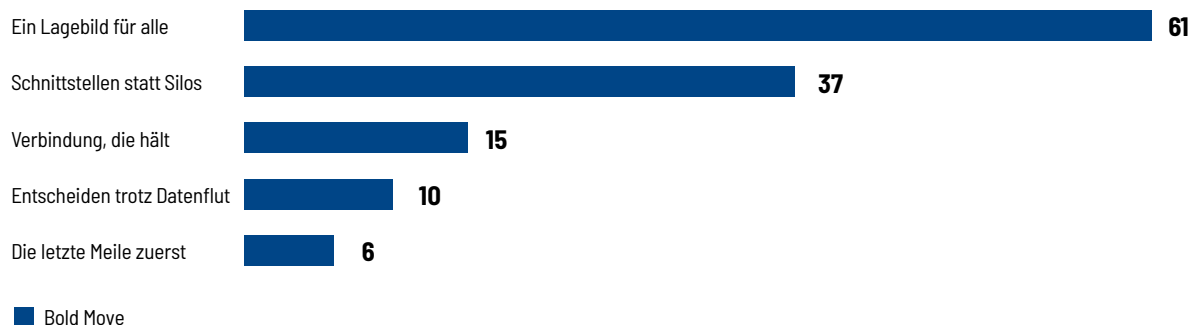
QUICK WIN Vorhandene Netze redundant verdichten

Statt neue Netze zu bauen, werden die vorhandenen so verdichtet, dass jeder Dienst einen zweiten Weg hat. Die BDBOS verdichtet den Digitalfunk, die Europäische Union stellt mit IRIS² eine satellitengestützte Verbindung bereit, die von der terrestrischen unabhängig ist. Hans-Martin Zimmermann verweist darauf, dass beide in Betrieb sind und sich weiter verdichten lassen.

Träger und Nachweis: Bund und Länder legen fest, welcher Dienst über welchen Weg läuft. Nach 24 Monaten liegt eine Rückfallmatrix je Dienst vor und ein satellitengestützter Pfad ist produktiv erprobt.

INFORMATION

Ein Handlungsfeld trägt fast ein Viertel aller Vorschläge



Handlungsfeld: Information & digitales Rückgrat · 129 Vorschläge

Abb. 7.2: Maßnahmen -Datenbank GSÖ 2030

Den föderierten Datenraum bauen, bevor die Daten fließen



Wer vor Ort handelt, braucht nicht alle Informationen, sondern die richtigen.

BOLD MOVE Einen föderierten Datenraum mit Rückkanal bauen.

Unternehmen und Behörden speisen ein und bekommen mehr zurück, als sie liefern. Der Rückkanal ist die Bedingung: Ohne ihn bricht die Beteiligung nach der ersten Krise ab. Der Datenbestand dient zugleich dem Training KI-gestützter Systeme. Genau diese Datengrundlage fehlt heute.



„Wenn ich mehr aus dem System herausbekomme, als ich hineingebe, dann mache ich aktiv mit – und dann bleibt das Gesamtsystem aktuell.“

Sven Hallbauer • Chief Revenue Officer,
EWERK Group

Träger und Nachweis: Das Bundesministerium des Innern beauftragt eine trägerneutrale Stelle als Betreiber, KRITIS-Betreiber und Länder speisen ein, der Rückkanal wird vertraglich zugesichert. Nach 24 Monaten läuft ein Mindestprodukt mit drei Sektoren.

BOLD MOVE Das zivil-militärische Lagebild aufbauen.

Zivile und militärische Lagebilder müssen verbunden werden, nicht in einem zentralen Bild zusammengeführt. Der Grund liegt in der Lage selbst: Verdichtet wird nur so weit, bis eine Entscheidung fällt, und nach oben gemeldet wird die Entscheidung, nicht der Rohbestand. Das Lagebild ist damit Privileg des Ausführenden, nicht des Entscheiders. Was fehlt, ist kein weiteres Lagebild, sondern ein Verzeichnis, aus dem sich der Ausführende holt, was er braucht.

Ein Vorhaben existiert bereits: das Ressortübergreifende Lagebild (RessüLa) der Bundeswehr. Es deckt heute die Logistik ab und könnte

als Basis dienen. Entscheidend ist die Reihenfolge: erst Prozesse, Zuständigkeiten und Berechtigungen klären, dann die Technik bauen. Dazu gehört auch die personelle Verfügbarkeit im Ernstfall.

Träger und Nachweis: Verteidigungsministerium und Planungsamt geben Mandat und Budget, Ressorts und Länder benennen Einspeisepflichten. Nach 24 Monaten sind drei Ressorts und drei Länder angebunden.

Zusammen verkürzen die fünf Maßnahmen die Zeit zwischen Ereignis und gemeinsamem Lagebild. Eines leisten sie nicht.

NEW HORIZON Die Lage von außen sehen

Neben das nachlaufende Lagebild gehört ein vorlaufendes. Satellitenaufklärung und die Sensorik an Flüssen und Talsperren zeigen eine Lage, bevor die erste Meldung eingeht – Christian Miller von der Feuerwehr Köln fordert genau das. Bisher entsteht das Bild auf Bundesebene ausschließlich aus Meldungen. Die Daten existieren, nur nicht standardisiert und zusammengeführt. Wer das beauftragt, ist die Frage des nächsten Handlungsfeldes.

7.3 – DIE STEUERUNG

Governance unterhalb der großen Reform beginnen

Im Handlungsfeld Governance, Recht und Steuerung wird geregelt, wer im Ernstfall führt, handeln darf und Mittel freigibt. Kapitel 4 hat gezeigt, dass hier die größte Lücke klafft. Von den 80 Vorschlägen aus 36 Interviews sind 13 sofort umsetzbar – beim Geld kein einziger.

Fünf Maßnahmen verlagern Entscheidungen aus der akuten Lage in die Vorbereitung. Drei Quick Wins schaffen Vorentscheidungen: Sie definieren den Zuständigkeitsübergang, richten Begegnungsräume ein und ziehen den Anwendungsfall vor die Governance-Klärung. Zwei Bold Moves machen daraus Führung: ein Stab mit Vollzeitkräften und eine Architektur, die zentral steuert und dezentral entscheidet. Keine davon verlangt eine Strukturreform.

QUICK WIN Den Zuständigkeitsübergang definieren

Wann eine Lage vom Landrat ins Innenministerium wechselt, steht nirgends. Norbert Ahrend von Arvato Systems nennt die Regel, die in der Praxis kursiert: Ab drei betroffenen Landkreisen übernimmt das Land. Geschrieben steht sie nicht, und die Klärung kostet im Ernstfall mindestens einen Tag. Ein ähnlicher Bruch besteht eine Ebene höher zwischen den Nachrichtendiensten und dem BSI.

Träger und Nachweis: Die Innenministerien von Bund und Ländern legen Schwellen und Auslöser schriftlich fest. Nach zwölf Monaten liegt für jedes Land eine Übergangsregel vor.

QUICK WIN Räume schaffen, in denen sich Akteure begegnen dürfen

Bundeswehr, Nachrichtendienste und Polizei arbeiten getrennt, und das Trennungsgebot bleibt. Für den regelmäßigen fachlichen Austausch unterhalb der Rechtsfrage fehlt ein Format. Christian Hummert

von der Cyberagentur kennt derzeit genau einen Ort, an dem diese Fachleute zusammenkommen.

Träger und Nachweis: Das Bundesministerium des Innern richtet ein turnusmäßiges Format ein, die Cyberagentur trägt es fachlich. Nach zwölf Monaten haben vier Treffen stattgefunden und eine gemeinsame Auswertung liegt vor.

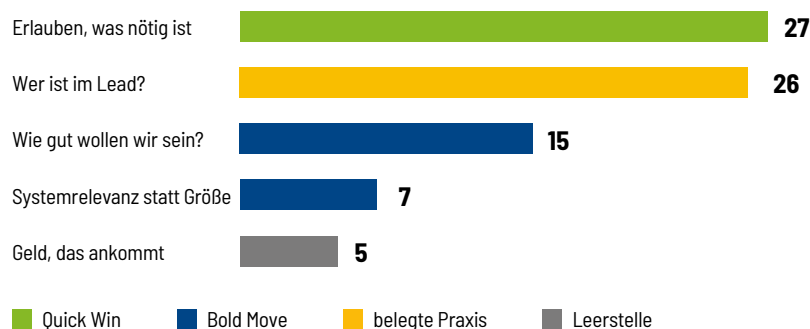
QUICK WIN Erst den Anwendungsfall bauen, dann die Governance klären

Die übliche Reihenfolge lähmt: Zuständigkeit, Rechtsrahmen und Betriebskonzept sollen stehen, bevor etwas entsteht. Dennis Ruf von conet verweist auf die Praxis in Unternehmen, die bei der Einführung Künstlicher Intelligenz umgekehrt vorgehen und Compliance am laufenden Fall klären. Auf den Staat gemünzt heißt das: erst eine funktionierende Lösung bauen – die Daten sind vorhanden und müssen nicht vollständig sein –, dann klären, welche rechtlichen weißen Flecken nachzuziehen sind. Das wäre das Signal an den Gesetzgeber.

Träger und Nachweis: Das Bundesministerium des Innern benennt zwei Anwendungsfälle aus dem laufenden Aufbau und setzt sie ohne Vorabklärung um. Nach zwölf Monaten laufen beide, und die Regelungslücke ist benannt.

GOVERNANCE

Fünf Vorschläge zum Geld, keiner davon umsetzbar



Handlungsfeld: Governance, Recht & Steuerung · 80 Vorschläge · 5 Cluster · 15,1 Prozent · 36 von 55 Interviews

Abb. 7.3: Maßnahmen-Datenbank GSÖ 2030

Zuständigkeit klären, bevor die Lage sie erzwingt



Wer im Ernstfall führt, muss vorher am Tisch gesessen haben.

BOLD MOVE Führung mit Vollzeitkräften einrichten

Krisenstäbe werden aus dem laufenden Betrieb heraus besetzt und üben selten. Tobias Schönherr von der Bundespolizei nennt Hessen als Vorbild: acht Vollzeit-Krisenführer, die immer zu zweit arbeiten und das ganze Jahr über auf solche Lagen vorbereitet sind. Die Einsatzführungsstäbe in Nordrhein-Westfalen sind eine zweite Referenz. Für den Bund fordert er keine neue Behörde, sondern ein klares Mandat für das, was bereits existiert.

Träger und Nachweis: Der Bund richtet einen solchen Stab ein, die Länder entsenden Verbindungspersonen, und die Mittelfreigabe wird an entscheidungsfähige Gremien delegiert statt kleinteilig vorgeschrieben. Nach 24 Monaten ist der Stab besetzt und hat zwei Übungen absolviert.

BOLD MOVE Zentral steuern, dezentral entscheiden

Wer alles über eine Stelle steuern will, geht in zigtausenden Anwendungsfällen unter. Die Alternative ist Modularität: Der Gesetzgeber verpflichtet einzelne Betreiber zu definierten Beiträgen, BSI und BBK definieren die Schnittstellen zwischen den Modulen. Dazu gehört, Bundesnetzagentur sowie Energie- und Luftfahrtaufsicht gesetzlich zur Bedrohungsvorsorge zu verpflichten. Heute steht das in keinem Aufgabenkatalog.

Zentrale Koordinierung bleibt notwendig, wo es um essentielle Güter und Leistungen geht. Gemeint ist der Bürokratie-Overhead, der Verantwortung von denen genommen hat, die sie tragen sollten.

Träger und Nachweis: Der Gesetzgeber schafft die Pflichten, BSI und BBK setzen die Schnittstellen. Nach 24 Monaten laufen drei Module produktiv, ohne zentrale Instanz.

Zusammen verlagern die fünf Maßnahmen die Entscheidung nach vorn. Eine Frage bleibt offen.

NEW HORIZON Klären, wer die dezentrale Struktur bezahlt

Je weiter unten in der Verwaltungsebene, desto größer der Haushaltsdruck – finanziert wird, was man tun muss, nicht, was man könnte. Marlis Cremer von den DRK-Kreisverbänden Düren und Jülich würde im Zweifel selbst die marode Schule sanieren statt die Sirene aufzubauen. Fünf Interviews fordern deshalb mehr Mittel für die dezentrale Struktur und einen Ausgleichsfonds für kommunale Folgen von Bundesentscheidungen. Einen Träger dafür benennt niemand.

7.4 – DIE RESSOURCEN

Beschaffungstempo aus vorhandenen Verträgen holen

Im Handlungsfeld Ressourcen, Industrie und Innovation entscheidet sich, wie schnell beschafft werden kann, wer im Ernstfall arbeitet und was im eigenen Land herstellbar bleibt. Die 85 Vorschläge verteilen sich fast gleichmäßig auf fünf Themen.

Fünf Maßnahmen nutzen Vorhandenes. Drei Quick Wins holen Tempo aus dem Bestand: Sie öffnen Rahmenverträge, behandeln Verbrauchsgüter wie Großgerät und ersetzen 400 Einzelgespräche durch einen Meldekanal. Zwei Bold Moves sichern die Grundlage: ein Transitplan für die zivile Infrastruktur und eine Cloud-Doppelstrategie. Vier davon stärken die wirtschaftliche Resilienz, die fünfte das digitale Rückgrat.

QUICK WIN Vorhandene Rahmenverträge öffnen

Die Bundeswehr hat Rahmenverträge, andere Behörden schreiben vergleichbare Leistungen neu aus. Frank Scholz von MilDef, dessen Unternehmen von genau diesen Ausschreibungen lebt, sieht hier den größten Hebel: Öffnet man die Verträge für andere Behörden mit Sicherheitsauftrag und für befreundete Streitkräfte, entsteht ein fortschreibbarer Katalog anstelle einer starren Ausschreibung über drei Jahre. Kommunale und kleine Anbieter müssen dabei mitgedacht werden – sie fallen heute durch das Raster, weil sie im ursprünglichen Beschaffungskonzept nicht als Bedarfsträger vorgesehen waren. Die Öffnung wirkt allerdings nur einmal. Der Engpass ist das Verfahren selbst. Wichtiger als die Öffnung ist deshalb die Vorfristigkeit: nicht Stückzahlen beschaffen, sondern Fertigungskapazität vertraglich sichern. MilDef investiert heute Millionen in Material und Infrastruktur auf Basis von Annahmen – ohne Stückzahlen, ohne Vertrag.

Träger und Nachweis: Das Beschaffungsamt der Bundeswehr öffnet die Verträge, Innen- und Finanzministerium regeln die Abrechnung. Nach zwölf Monaten sind mindestens drei Rahmenverträge behördenübergreifend nutzbar und die Beschaffungsdauer im Pilotfall halbiert.

QUICK WIN Verbrauchsgüter behandeln wie Großgerät

Neues Gerät findet den Weg in den Haushalt, Munition und Verbrauchsmaterial nicht – ein Kampfpanzer hat Munition für etwa einen Tag, wie Peter Kuhne von der IHK Bonn/Rhein-Sieg vorrechnet. Ein Beispiel aus der Praxis: Eine zweite Verpackungsform für rund 20.000 Euro wird seit Langem nicht finanziert, obwohl sie die Ausbringung verdoppeln würde.

Träger und Nachweis: Das Verteidigungsministerium priorisiert Verbrauchsgüter im Haushalt wie Großgerät, das Beschaffungsamt finanziert Werkzeuge und Formen beim Zulieferer. Nach zwölf Monaten ist die Bevorratung mit einem Reichweitenziel hinterlegt.

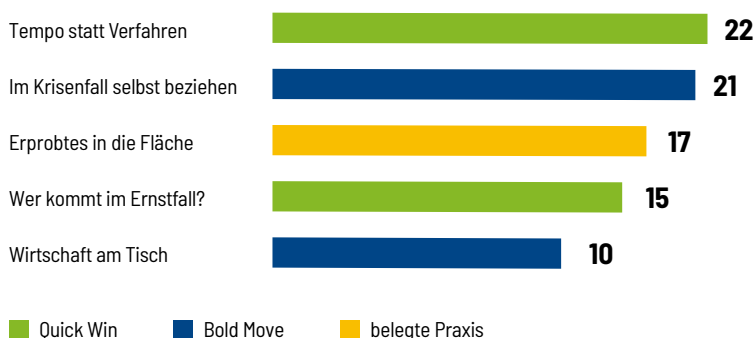
QUICK WIN Einen Meldekanal statt vierhundert einrichten

Hanno Friedrich von der Kühne Logistics University nennt den Fall: In der Pandemie musste ein Lebensmitteleinzelhändler mit 400 Kreisen einzeln sprechen. Eine Plattform, über die Unternehmen Störungen melden und die betroffenen Stellen aufbereitete Lagen zurückbekommen, ersetzt diese Gespräche. Ergänzend binden die Ressortoberbehörden die Betreiber kritischer Infrastruktur über Verbindungspersonen an.

Träger und Nachweis: Das Wirtschaftsministerium betreibt die Plattform, das BBK wertet aus. Nach zwölf Monaten sind drei Sektoren angeschlossen.

RESSOURCEN

Fünf Themen, und keines ist der eine Hebel



Handlungsfeld: Ressourcen · 85 Vorschläge

Abb. 7.4: Maßnahmen-Datenbank GSÖ 2030

Die Infrastruktur ertüchtigen, bevor sie gebraucht wird



Werkzeuge und Formen entscheiden über das Tempo. Finanziert werden sie selten.

BOLD MOVE Die zivile Infrastruktur auf Transit auslegen

Armin Schaus vom Operativen Führungskommando der Bundeswehr nennt die Größenordnung: Bis zu 800.000 Kräfte sollen binnen eines halben Jahres durch Deutschland an die Ostflanke verlegt werden. Militärtransporte wiegen dabei statt 30 heute 60 bis 80 Tonnen, Häfen und Umschlagpunkte fehlen. Begründen lasse sich die Ertüchtigung nicht allein militärisch – die Exportnation brauche sie ohnehin. Ungeklärt ist die Haftung. Wer zahlt, wenn eine Brücke unter Überlast bricht – Kommune, Land, das deutsche Militär oder der Bündnispartner, gegen den womöglich kein Regress besteht? Rainer Sommer von der Provinzial erwartet den größten Zeitverlust bei der Schuldfrage, nicht bei der Reparatur.

Träger und Nachweis: Verkehrs- und Verteidigungsministerium stimmen einen gemeinsamen Bedarfsplan ab und klären die Haftung vorab. Militärische Bedarfe fließen bereits in die Verkehrsplanung ein, Baumaßnahmen lassen sich für den Operationsplan priorisieren. Nach 24 Monaten liegt beides vor.



„Im Frieden für den Krieg beschaffen – man muss vom Ziel 2030 rückwärts rechnen, nicht vorwärts.“

Frank Scholz • Geschäftsführer, MilDef

BOLD MOVE Eine Cloud-Doppelstrategie fahren

Vollständige Abhängigkeit von einem Anbieter ist riskant, vollständiger Verzicht auf verfügbare Leistung ebenso. Christian Marwitz von der

BWI beschreibt den Ausweg als Multi-Cloud-Ansatz aus mehreren, gegeneinander absicherbaren Bausteinen: die Variante eines großen Anbieters im eigenen Rechenzentrum und eine selbst entwickelte offene Architektur, die auf kompakter Hardware läuft und bis ins Fahrzeug verlegt werden kann.

Träger und Nachweis: Die BWI betreibt beide, das Verteidigungsministerium entscheidet je Anwendung. Nach 24 Monaten ist eine Kritikalitätsmatrix beschlossen und eine verlegefähige Instanz im Feld erprobt.

Zusammen holen die fünf Maßnahmen Tempo aus bestehenden Strukturen. Eines lässt sich so nicht beschleunigen.

NEW HORIZON Forschung schützen, bevor sie abfließt

Christian Hummert von der Cyberagentur nennt die Forschungssicherheit seine größte Sorge: Sicherheitsforschung finde in normalen Besprechungsräumen einer Universität statt, in denen auch ausländische Studierende ein und aus gehen, und Start-ups bauen Waffensysteme, ohne dass der Umgang mit dem Wissen geklärt wäre. Dänemark und weitere skandinavische Länder haben ein Modell dafür: geschlossene Räume, gesicherte Arbeitsplätze, überprüfbares Personal, eine beratende Stelle. Das ließe sich übernehmen.

7.5 – DER SCHUTZ

Objektschutz und Cyberabwehr zusammendenken

Im Handlungsfeld Schutz und Abwehr geht es um physische und digitale Angriffe. Mit 58 Vorschlägen ist es das kleinste Feld der Studie und das mit der schärfsten Trennlinie: Sicherheitsleitstände und Objektschutz arbeiten nebeneinander her und gehen beide vom isolierten Angriff aus.

Fünf Maßnahmen schließen die Kette von der Erkennung bis zur Ausführung. Drei Quick Wins wirken am Ort des Angriffs: Sie holen die KRITIS-Betreiber ins Cyber-Lagebild, härten die Kliniken und üben Reaktionsketten für niederschwellige Sabotage. Zwei Bold Moves verbinden, was heute getrennt läuft – physische Lage und Cyberlage, Erkenntnis und Entscheidung. Zwei davon stärken den Schutz kritischer Infrastrukturen, drei die Abwehrfähigkeit.

QUICK WIN Die KRITIS-Betreiber ins Cyber-Lagebild holen

Über die Bedrohungslage wird debattiert, statt sie zu vermessen. Dabei existiert sie längst. Thomas Tschersich von der Deutschen Telekom beziffert sie auf dezentral hundert Prozent und zentral null: Energieversorger, Telekommunikationsbetreiber und Wasserwirtschaft haben jeder ihr eigenes Lagebild, ein gemeinsames gibt es nicht. Das nationale Cyberabwehrzentrum bestehe, sagt er, nur seien die Betreiber nicht eingeladen – obwohl sie die wesentlichen Teile mitbringen. Ein Format zeigt, wie es ginge: Cyber Nation Germany baut mit dem BSI eine Lage für die 40 größten deutschen Unternehmen auf, mit Treffen viermal im Quartal.

Träger und Nachweis: Das Format wird über die Börsenwerte hinaus auf die Betreiber kritischer Infrastruktur geöffnet, die Betreiber entsenden Verbindungspersonen in das Lagebildgremium. Nach zwölf Monaten speisen drei weitere Sektoren ein.

QUICK WIN Krankenhäuser härten

Zugangskontrollen fehlen, Notstrom ist knapp bemessen, die Informationstechnik ist der verwundbarste Punkt – Jahrzehnte des Investitionsstaus haben Kliniken angreifbar gemacht. Wie weit die Maßstäbe auseinanderliegen, zeigt eine Episode, die Leif Erik Sander von der Charité erzählt: Kollegen eines israelischen Medizinzentrums, eingeladen, das Haus zu begutachten und ein Weißbuch zu erstellen, fragten als Erstes nach dem Flugabwehrsystem – in einer Klinik, die nicht einmal Zugangskontrollen leisten kann.

Träger und Nachweis: Länder und Träger legen ein Härtingsprogramm auf, das BSI gibt den Mindeststandard vor. Nach zwölf Monaten ist für jedes Haus der Versorgungsstufe eins ein Härtingsplan hinterlegt.

QUICK WIN Auf niederschwellige Sabotage reagieren können

Michael Kreinest von den BG Kliniken nennt drei Fälle derselben Größenordnung: eine Spielzeugdrohne, zwei durchtrennte Kabel, ein Brandanschlag. Die Kabel stoppen eine ICE-Strecke über Tage, der Brandanschlag legt einen Stadtteil lahm. Für diese Größenordnung gibt es weder Zuständigkeit noch eingeübte Reaktion, und sie wird zunehmen.

Träger und Nachweis: Die Länder benennen für jede Kategorie eine erstalarmierte Stelle, der Bund stellt die Fähigkeit zur Abwehr unbemannter Systeme bereit. Nach zwölf Monaten liegt für drei Fallgruppen eine geübte Reaktionskette vor.

SCHUTZ

Fünf von 58 Vorschlägen betreffen das Entscheiden



VORSCHLÄGE NACH WIRKUNGSVERSPRECHEN



Handlungsfeld: Schutz & Abwehr · 58 Vorschläge

Abb. 7.5: Maßnahmen-Datenbank GSÖ 2030

Erkennen ohne Entscheidungsbefugnis bleibt folgenlos



Ein Team, das bereitsteht, entscheidet schneller als eines, das zusammengerufen wird.

BOLD MOVE Physische Lage und Cyberlage zusammenführen

Wer von isolierten Angriffen ausgeht, übersieht den kombinierten. Ein nationales Vorhaben, beide Lagen systematisch zusammenzuführen, gibt es nicht – nur eine Ausschreibung der NATO. Auch Gegenmaßnahmen müssen beide Bereiche berücksichtigen.

Träger und Nachweis: Das BSI und das BBK verknüpfen beide Lagen, Betreiber melden über einen Kanal, die Bundeswehr bringt ihre NATO-Erfahrung ein. Nach 24 Monaten läuft eine korrelierte Auswertung, erste Fälle sind dokumentiert.



„Dass ein Cyberangriff mit einer physischen Bedrohung verbunden wird, hat man nicht auf dem Radar.“

Hans-Martin Zimmermann • Head of Engineering Defence Digital, Airbus Defence and Space

BOLD MOVE Dem Cyber-Krisenstab ein Mandat geben

Bernd König von Google Cloud schlägt den Ausbau statt der Neugründung vor: Das nationale Cyberabwehrzentrum im BSI bündelt Fachwissen, nicht Entscheidungsmacht – ein einzelner Vertreter der Bundeswehr kann dort wenig mehr tun als telefonieren. Mit Mandat, Mitteln und Personal könnte das Zentrum ministerielle Zuständigkeiten im Krisenfall überbrücken. Die rechtlichen Ansatzpunkte liegen bei Bundeskriminalamt, Bundespolizei und BSI: Umleitung von Datenverkehr, Unterbrechung von Datenströmen, gestaffelte Eingriffsschwellen mit Richtervorbehalt.

Mit dem Gemeinsamen Zentrum zur Abwehr hybrider Bedrohungen ist seit Juni 2026 ein zweiter Ansatz im Aufbau. Die Mandatsfrage stellt sich dort genauso.

Träger und Nachweis: Das Bundesministerium des Innern legt den Gesetzentwurf vor. Nach 24 Monaten ist das Mandat gesetzlich verankert.

Zusammen machen die fünf Maßnahmen aus der Erkenntnis eine Entscheidung. Eine Quelle bleibt dabei noch ungenutzt.

NEW HORIZON Die Bevölkerung als Sensor

In der Ukraine melden Bürgerinnen und Bürger über Anwendungen Drohnen und Menschen in Not. Lokale Beobachtungen von Passanten, Polizisten und Drohnen laufen zentral zu einem Bild zusammen. Geschwindigkeit entsteht dort aus Beteiligung. Offen bleiben die Zuständigkeiten: Über welche Kanäle gehen Meldungen ein, und wer antwortet darauf?

7.6 – DIE RESILIENZ

Was zuerst wieder anläuft, muss vorher feststehen

Im Handlungsfeld Resilienz und Versorgung geht es darum, einen Treffer zu überstehen und danach wieder anzulaufen. Mit 113 Vorschlägen ist es das zweitgrößte Feld der Studie. Von allen 529 Vorschlägen betreffen jedoch nur 19 die Phase nach der Krise.

Fünf Maßnahmen bilden eine zeitliche Kette. Drei Quick Wins wirken vor der Lage: Sie klären die Betankungsreihenfolge, machen den Wiederanlauf planbar und sagen der Wirtschaft, was geplant ist. Zwei Bold Moves sichern, was im Verteidigungsfall wegbricht: vertraglich gebundene Hilfsorganisationen und eine nicht-militärische CBRN-Einheit. Drei davon stärken die Resilienz kritischer Infrastrukturen, zwei die wirtschaftliche Resilienz.

QUICK WIN Die Betankungskette vom Netz bis zum Hof durchdenken
Notstrom hält, solange Diesel nachkommt – und wer zuerst betankt wird, ist nirgends festgelegt. Thomas Tschersich von der Deutschen Telekom stellt die Frage über 50 bis 60 Szenarien hinweg: Krankenhaus, Wasserwerk oder Netz? Für den Digitalfunk gibt es eine Antwort. Thomas Scholle von der BDBOS beschreibt 72 Stunden Härting und danach ein mit dem Technischen Hilfswerk abgestimmtes Betankungskonzept. Kommerzielle Standorte dagegen puffern ein bis zwei Stunden, dann brauchen sie Diesel. Und in der Fläche fehlt dezentrale Ersatzenergie: 93.000 Milchkühe im Landkreis Friesland lassen sich nicht von Hand melken.

Träger und Nachweis: Betreiber melden ihren Bedarf, Land und Technisches Hilfswerk legen die Reihenfolge fest. Nach zwölf Monaten ist sie je Kreis dokumentiert und einmal geübt.

QUICK WIN Den Wiederanlauf beherrschbar machen
Der Wiederanlauf dauert länger als der Ausfall und läuft weitgehend von Hand. Papierne Wiederanlaufzeiten halten der Realität nicht stand – dokumentiert sind 60 Minuten, tatsächlich vergingen 48 Stunden. Zielzustand ist nicht der Ursprungszustand, sondern eine belastbare

Übergangslösung: erst das Pflaster, dann der Neubau.

Träger und Nachweis: Die Träger erstellen einen Wiederanlaufplan, das Land verankert ihn als Auflage im Krankenhausplan. Nach zwölf Monaten hat jedes Haus der Maximalversorgung einen dokumentierten und einmal geübten Plan.

QUICK WIN Der Wirtschaft sagen, was geplant ist

Unternehmen können sich nicht vorbereiten, solange sie Verlegewege, Sammelplätze und benötigte Gebäude nicht kennen – und ohne diese Kenntnis bekommen sie intern keine Mittel frei. Der Informationsaustausch muss in beide Richtungen funktionieren. Die Versicherungswirtschaft gehört neben den Banken zu den größten Datenverarbeitern des Landes. Sie betreibt doppelt abgesicherte Rechenzentren in Deutschland und verfügt über Geodaten sowie Wettermodelle, die sich unter einem Vertraulichkeitsrahmen in ein nationales Lagebild einspeisen ließen.



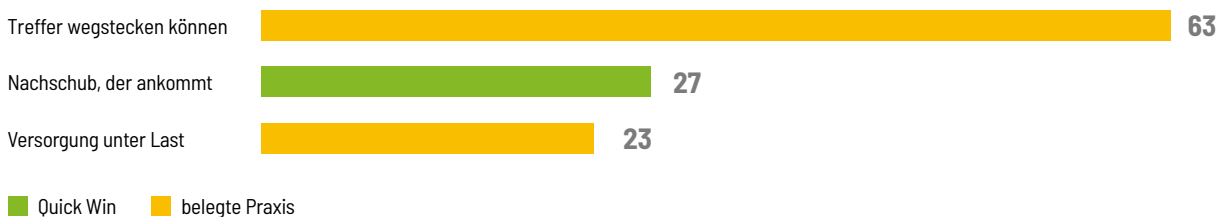
„Wir sitzen in einem Boot – die Verteidigung, das Innenministerium und die Wirtschaft.“

Dr. Rainer Sommer • Vorstand, Provinzial Holding

Träger und Nachweis: Das Operative Führungskommando definiert freigebbare Auszüge aus dem Operationsplan, die Landeskommmandos übermitteln sie an Betreiber und Kammern, der Staat benennt zugleich seinen Bedarf an ziviler Kapazität. Nach zwölf Monaten steht ein Informationskatalog und mindestens 100 Unternehmen entlang der West-Ost-Achse sind informiert.

RESILIENZ

Nur jeder zehnte Vorschlag geht auf den Wiederanlauf



Handlungsfeld: Resilienz & Versorgung · 113 Vorschläge

Abb. 7.6: Maßnahmen-Datenbank GSÖ 2030

Wer einspringt, wenn die Bundeswehr gebunden ist



Das gesellschaftliche Verhalten entscheidet, lange bevor die Technik greift

BOLD MOVE Zivil-militärische Kooperation vertraglich binden

Im Verteidigungsfall steht die Bundeswehr für zivile Aufgaben nicht zur Verfügung, und die Hilfsorganisationen übernehmen Aufgaben, für die sie keinen Auftrag haben. Ein Weg ist vorgezeichnet: In einem Kooperationsvertrag mit dem Sanitätskommando ist vorgesehen, dass die Hilfsorganisationen den Rücktransport Verwundeter übernehmen. Geübt wurde er bereits – Kapitel 4 beschreibt die Übung an der zivil-militärischen Schnittstelle.

Träger und Nachweis: Das Sanitätskommando schließt Rahmenverträge auch mit dem Deutschen Roten Kreuz, die Länder erklären die Freistellung der Ehrenamtlichen. Nach zwölf Monaten ist der Vertrag unterzeichnet und einmal geübt.

BOLD MOVE Eine nicht-militärische CBRN-Einheit des Bundes aufbauen

Fällt die Bundeswehr als ziviler Helfer aus, fehlt für chemische, biologische, radiologische und nukleare Lagen der Träger. Tobias Schönherr von der Bundespolizei verweist auf die Risikoanalyse des Bundesamtes für Bevölkerungsschutz vom Januar 2026, die genau diese Lücke benennt.

Träger und Nachweis: Technisches Hilfswerk und Bundespolizei bilden gemeinsam eine Einheit, die diese Aufgabe im Verteidigungsfall trägt. Nach 24 Monaten ist sie aufgestellt, ausgestattet und einsatzbereit.

Zusammen decken die fünf Maßnahmen die Zeit vor und während der Lage ab. Für die Zeit danach fehlt die Übung.

NEW HORIZON Den Wiederanlauf simulieren, weil er sich nicht proben lässt

Ein Blackout lässt sich real nicht üben. Bernd Calaminus von EnBW beschreibt einen Simulator, an dem sich genau das trainieren lässt – vom schrittweisen Netzwiederaufbau bis zur Reihenfolge der Verbraucher. Im Interviewkorpus ist er die einzige belegte Antwort auf die Frage, wie man für eine Lage übt, die sich nicht herstellen lässt.

7.7 – DIE GESELLSCHAFT

Wer führen soll, muss es geübt haben

Im Handlungsfeld Gesellschaft, Kultur und Üben geht es um die Menschen, die im Ernstfall mitwirken sollen: Bevölkerung, Ehrenamt, Verwaltung und politische Entscheidungsträger. Mit 64 Vorschlägen wird die gesellschaftliche Dimension breit gefordert, aber dünn ausbuchstabiert.

Fünf Maßnahmen setzen bei denen an, die führen sollen. Drei Quick Wins befähigen die Verantwortlichen: Sie bringen die entscheidende Ebene ins Üben, verankern Krisenmanagement in der Verwaltungsbildung und lassen Nachbarschaften über Landesgrenzen hinweg entstehen. Zwei Bold Moves schaffen auf Bundesebene die Voraussetzungen: eine Innenperspektive im Nationalen Sicherheitsrat und eine bundesweite Erhebung von Katastrophendaten.

QUICK WIN Üben, wer im Ernstfall entscheidet

Die Übung muss die Ebene erreichen, die im Ernstfall entscheidet – von der Kommune über die Bezirksregierung bis zum Land, mit den politischen Verantwortlichen am Tisch. Heute ist es umgekehrt. Die länderübergreifende Krisenmanagementübung LÜKEX findet ohne politische Entscheidungsträger statt: Geübt wird die Ebene darunter, entschieden wird oben. Marlis Cremer von den DRK-Kreisverbänden Düren und Jülich nennt LÜKEX die einzige Übung, die wenigstens bis auf die Länderebene hinunterreicht. Was fehlt, ist die verbindliche Verpflichtung zum regelmäßigen Üben – für politische Amtsträger ist sie inzwischen angekündigt.

Träger und Nachweis: Die Innenministerien der Länder verpflichten Krisenstabsleitungen und kommunale Hauptverwaltungsbeamte zu Übung und Fortbildung. Nach zwölf Monaten hat jedes Land eine ebenenübergreifende Übung mit politischer Beteiligung durchgeführt.

QUICK WIN Krisenmanagement in die Verwaltungsbildung aufnehmen

Krisenmanagement wird verpflichtender Bestandteil der Ausbildung, von der Hochschule für Polizei und öffentliche Verwaltung bis zur Angestelltenausbildung. Wer heute eine Lage führen soll, hat es nie gelernt. Der Fachkundenachweis für Landräte ist ein Anfang, operative Leitungen und kommunale Stäbe bleiben außen vor. Voraussetzung ist eine Fehlerkultur. Nach dem bundesweiten Warntag wurde die Leitung ausgetauscht, statt die Fehlerquelle zu bearbeiten.

Träger und Nachweis: Die Länder ändern die Ausbildungsordnungen, der Aufwand ist gering. Nach zwölf Monaten ist es in einem Land verankert.

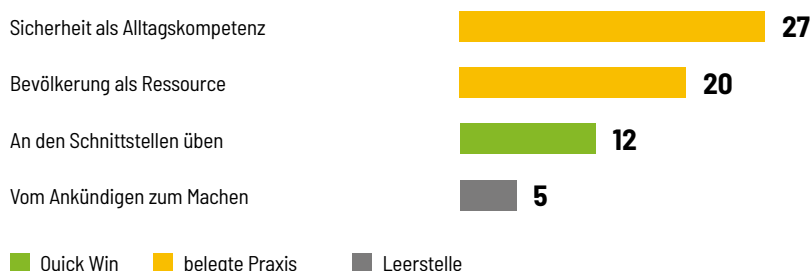
QUICK WIN Nachbarschaft über die Landesgrenze organisieren

Kreise organisieren ihre Zusammenarbeit über die Landesgrenze hinweg, und die Rettungsleitstelle darf Bundeseinheiten direkt rufen, statt über Landrat und Innenministerium zu eskalieren. Dass das trägt, zeigt Volker Lemgen von der Kreisverwaltung Neuwied: Sein Kreis und der Rhein-Sieg-Kreis arbeiten über die Grenze zwischen Rheinland-Pfalz und Nordrhein-Westfalen zusammen, mit ständigem Austausch, gegenseitiger Fortbildung und unkomplizierter Anforderung von Kräften. Brände halten an Landesgrenzen nicht an.

Träger und Nachweis: Die Länder erlauben die direkte Alarmierung. Nach zwölf Monaten bestehen fünf solcher Nachbarschaften.

GESELLSCHAFT

Über die Umsetzung wird geredet, vorgeschlagen wird sie nicht



Handlungsfeld: Gesellschaft, Kultur & Üben • 64 Vorschläge

Abb. 7.7: Maßnahmen-Datenbank GSÖ 2030

Bevölkerung als Key Player mitdenken



Wer beteiligt wird, wartet nicht auf Hilfe.

BOLD MOVE Den Nationalen Sicherheitsrat nach innen öffnen

Der Nationale Sicherheitsrat bekommt die Innenperspektive. Er arbeitet seit dem 1. Januar 2026 und ist außen- und sicherheitspolitisch ausgerichtet. Der Bevölkerungsschutz nach innen kommt darin nicht vor, und damit fehlt dem Gremium die Gesamtstaatlichkeit, die sein Name verspricht. Frank Weber vom Zukunftsforum Öffentliche Sicherheit benennt die Lücke. Gemeint ist nicht der Zivilschutz, der erst im Verteidigungsfall greift, sondern das Versagen staatlicher Funktionen – das droht auch bei einem großen Angriff auf die Versorgungsinfrastruktur.

Träger und Nachweis: Das Bundeskanzleramt erweitert Geschäftsordnung und Besetzung um die Innenperspektive, die Länder benennen eine gemeinsame Vertretung. Nach 24 Monaten steht der Bevölkerungsschutz regelmäßig auf der Tagesordnung.

BOLD MOVE Katastrophendaten bundesweit erheben

Bund und Länder erheben Katastrophendaten nach einem gemeinsamen Raster. Heute fehlt es daran: Das internationale Sendai-Rahmenwerk verlangt Dutzende Indikatoren – wie viele Menschen in Katastrophen sterben, wie lange es nach einem Ausfall dauert, bis kritische Infrastruktur wieder läuft. Benni Thiebes vom Deutschen Komitee Katastrophenvorsorge kann dazu kaum belastbare Zahlen berichten, weil jedes Land nach eigenen Regeln sammelt. Ohne diese Daten lässt sich weder sagen, ob Vorsorge wirkt, noch wo sie fehlt.

Träger und Nachweis: Bund und Länder einigen sich auf ein gemeinsames Erhebungsraster, das Bundesamt für Bevölkerungsschutz führt die Daten zusammen. Nach 24 Monaten liegt die erste voll-

ständige Erhebung vor.

Vier der fünf Maßnahmen richten sich an die Verwaltung, eine an den Bund. Die Bevölkerung kommt in keiner von ihnen als Handelnde vor.



„Bevölkerung müssen wir anders denken – sie ist für mich nach wie vor ein Key Player in dem ganzen Konzert.“

Martin Zeidler • Abteilungsleiter L, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

NEW HORIZON Aus Betroffenen Handelnde machen

Wer Resilienz aufbaut, hört den Vorwurf, er bereite Krieg vor. Der Einwand kursiert bereits, auch in kirchlichen Kreisen. Ansgar Rieks will ihn im Zentralkomitee der deutschen Katholiken friedensethisch klären. Den Vorwurf entkräftet am ehesten, wer die Bevölkerung nicht nur schützt, sondern beteiligt.

Das Bild, auf das die Gespräche hinauslaufen, ist ein anderes als das des geschützten Publikums: Der Staat redet offen über Risiken – auch darüber, dass im Ernstfall nicht allen zugleich geholfen werden kann – und traut den Menschen zu, sich als Gemeinschaft selbst zu helfen. Jeder weiß, was er beiträgt, ist dafür geschult und ausgestattet, und die Vorsorge für die ersten 72 Stunden steht im Regal, nicht nur in einer Broschüre.

Alle 30 Maßnahmen zeigen, wie ein handlungsfähiges gesamtstaatliches Sicherheitsökosystem entstehen kann. Der nächste Abschnitt stellt die Zielmarken für 2030 vor.

7.8 – DAS ZIEL

Festlegen, wie gut wir sein wollen

Deutschland arbeitet an seiner Sicherheitsarchitektur ohne Zielmarke. Ohne sie lässt sich weder sagen, ob die Richtung stimmt, noch wann genug getan ist. Kapitel 3 endete mit der Frage, die über alle weiteren entscheidet: Wie gut wollen wir sein? Dieser letzte Abschnitt liefert die Antwort.

Bis 2030 steht Deutschland dort, wo Estland heute steht: 25 von 30 Punkten im Systemreifegrad statt der heutigen 14. Neun Maßnahmen führen dorthin, je eine pro Dimension. Die zehnte Dimension trägt ein Entwicklungshorizont: Forschung schützen, bevor sie abfließt. Die Marke ist ambitioniert, aber realistisch, wenn jetzt die notwendigen Maßnahmen beschlossen werden.

Geführt wird nach geschriebenen Regeln. Eine Lage wechselt die Ebene nach einer festgelegten Schwelle, nicht nach einem Telefonat. Der Bund setzt Ziele und Schnittstellen, entschieden wird vor Ort. Und wer im Ernstfall entscheidet, hat es geübt – bis hinauf zur politischen Ebene.

Das Lagebild entsteht laufend, nicht auf Anforderung. Betreiber und Länder speisen ein, weil sie mehr zurückbekommen, als sie liefern. Eingestufte und offene Netze sind in beide Richtungen durchgängig. Und jeder Dienst hat einen zweiten Weg: Fällt das terrestrische Netz aus, trägt der Satellit.

Im Ernstfall greifen vorbereitete Ketten. Die Hilfsorganisationen haben einen Auftrag statt einer Bitte, der Wiederanlauf ist geplant und

geübt. Die Wirtschaft kennt Verlegewege, Sammelplätze und Bedarfe und kann Mittel dafür freigeben. Und die Sicherheitsforschung arbeitet in gesicherten Räumen, sodass Wissen im Land bleibt.

Drei dieser Maßnahmen wirken erst, wenn ihre Nutzung verpflichtend ist: Die Länder sind an das gemeinsame Lagebild angeschlossen, die Betreiber bekommen ihren Rückkanal vertraglich zugesichert, und die Wirtschaft erhält Planungsinformationen als Anspruch, nicht als Gefallen. Estland und die Niederlande haben genau so entschieden – das System und die Pflicht, es zu nutzen, im selben Beschluss.

Eine Zielmarke für die gesamtstaatliche Sicherheit lässt sich nur dort beschließen, wo die Ressortgrenzen enden: im Bundeskanzleramt, über den Nationalen Sicherheitsrat. Was dieser Beschluss braucht, ist eine Strategie im Zuschnitt dieses Zielbilds – Wirkung vor Zuständigkeit, eine Zielmarke je Dimension, ein Termin und ein Träger.

WEGMARKEN

Was jetzt entschieden wird, entscheidet, wo wir 2030 stehen

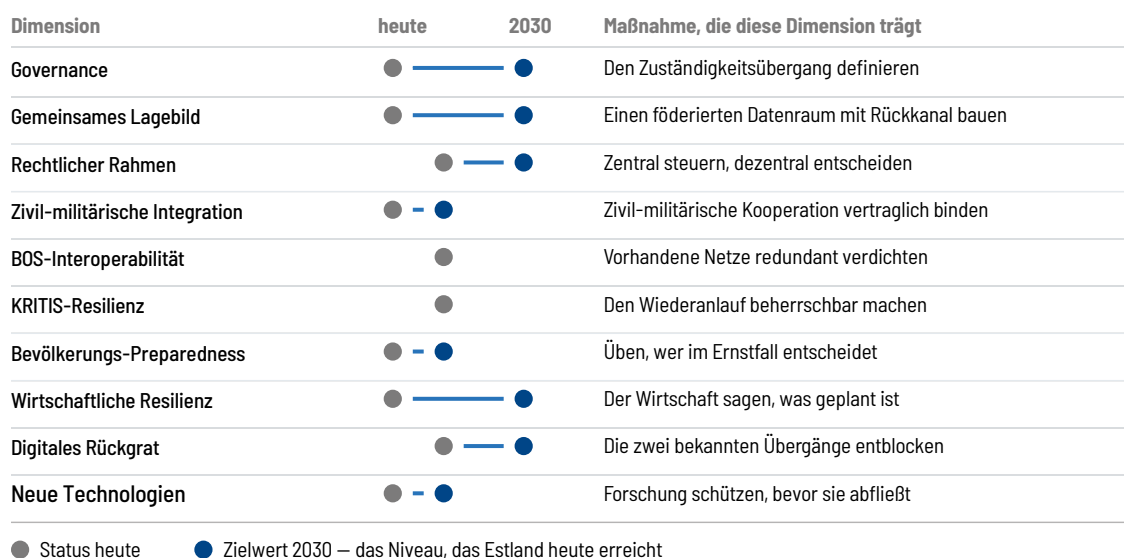


Abb. 7.8: Systemreifegrad-Benchmark

Epilog

EINLADUNG INS NETZWERK

Handlungsfähigkeit entsteht durch Verbindung

Diese Studie endet bei einer Aufgabe, die kein Ressort, keine Organisation und kein Unternehmen allein erledigen kann: Vorhandene Fähigkeiten müssen so verbunden werden, dass aus Lageinformationen Entscheidungen und aus Entscheidungen rechtzeitig Wirkung entsteht.

Dafür braucht Deutschland verbindliche Mandate, belastbare Übergaben und eine Praxis, die vor der Krise eingeübt wird. Die politischen und administrativen Entscheidungen liegen bei den zuständigen staatlichen Stellen.

AFCEA Bonn e.V. schafft die Brücke zwischen denen, die entscheiden, und denen, die Fähigkeiten bereitstellen, betreiben oder im Einsatz nutzen. Dieses Netzwerk war das Fundament der Studie. Das Partnermodell mit dreizehn Studienpartnern brachte unterschiedliche Perspektiven zusammen. Eine Befragung unter Technologieanbietern und Anwendern, 55 Tiefeninterviews sowie die Auswertung von Forschung, Regierungsberichten und Rechtsgrundlagen erweiterten das Bild.

Das Zielbild kanalisiert diese Perspektiven in eine gemeinsame Sprache: Lage erkennen, bewerten, entscheiden, koordinieren, handeln, durchhalten, wiederherstellen und lernen. Die verdichteten Vorschläge wurden anschließend gemeinsam mit den Partnern zu sechs Handlungsfeldern und konkreten Handlungssträngen priorisiert. Daraus entstanden

Maßnahmen mit Träger, Frist und überprüfbarem Nachweis. Die Studie liefert damit einen Arbeitsstand, an den politische, administrative, militärische und wirtschaftliche Entscheider anknüpfen können.

Wie eine solche Verbindung praktisch aussieht, zeigte CIMIC Quadriga 2026. Vom 14. bis 26. Juni übten in Niedersachsen Soldatinnen und Soldaten aus 28 Nationen gemeinsam mit Polizei, Feuerwehr, Hilfsorganisationen, Kliniken, Verwaltungen und Unternehmen. Mehr als 150 Lageeinspielungen bildeten unter anderem die Drehscheibe Deutschland im Bündnisfall ab. Eine zivile Spedition betrieb ein Convoy Support Center. Solche Regelformate machen Rollen, Abhängigkeiten und Übergaben sichtbar, bevor Zeitdruck sie erzwingt.

AFCEA Bonn e.V. hält dafür Gesprächs- und Arbeitsräume offen: zwischen Bundeswehr und Behörden, Bund, Ländern und Kommunen, Betreibern, Industrie, Wissenschaft und Hilfsorganisationen. Aus Kontakten sollen belastbare Verfahren werden, aus Pilotprojekten verfügbare Fähigkeiten und aus Übungen verbindliche Änderungen.

Wer an dieser Verbindung mitarbeiten will, ist eingeladen, Teil des AFCEA-Netzwerks zu werden.

Die Studienleitung

Anhang

Über diese Studie – Datengrundlage, Methodik und Quellen

ÜBER DIESE STUDIE

Datengrundlage

Diese Studie entstand in vier Stufen. Jede bereitete die nächste vor. Erkenntnisse aus externen Quellen wurden anschließend an eigenen Daten geprüft.

Am Anfang wertete die Studienleitung vorhandene Quellen aus.

Dazu gehörten Studien, Regierungsberichte, Rechtsgrundlagen und dokumentierte Krisenverläufe aus dem In- und Ausland, das Quellenverzeichnis ab Seite 116 führt sie einzeln auf, mit Güteklassifikation und Zuordnung zu den Abschnitten. Daraus entstanden zwei Werkzeuge: ein Benchmark, der den Systemreifegrad im Ländervergleich anhand von zehn Dimensionen misst, und eine Datenbank mit internationalen Beispielen. Sie zeigt, wie andere Staaten einzelne Übergänge gelöst haben.

Auf dieser Grundlage entstand ein erstes Zielbild. Es beschreibt, welche Fähigkeiten ein gesamtstaatliches Sicherheitsökosystem braucht und wie sie zusammenwirken müssen. Die Studienpartner prüften und überarbeiteten das Zielbild in drei Expertenworkshops vor der Erhebung. Dieser Rahmen half später, die Aussagen einzuordnen.

Erst danach begann die Erhebung in zwei parallelen Strängen. Die Studienleitung führte zwischen März und August 2026 55 Gespräche von jeweils rund 60 Minuten. Grundlage war ein einheitlicher Leitfaden. Zu jedem Gespräch entstand eine Zusammenfassung, die der Gesprächspartner zur Freigabe erhielt. Die Studie zitiert ausschließ-

lich aus diesen freigegebenen Fassungen. Parallel wurden Technologieanbieter und Anwender online befragt. Die Befragung endete am 14. Juni 2026 mit 72 auswertbaren Antworten.

Aus beiden Strängen gingen zwei Datenbanken hervor. Die erste erfasst 529 Vorschläge, die in Kapitel 7 zu 30 Maßnahmen gebündelt wurden. Die zweite erfasst 172 Lösungen, davon 131 aus den Gesprächen und 41 aus der Befragung. Die jeweilige Grundmenge ist entscheidend: Aussagen über Reife und Marktangebot stützen sich auf die 41 Befragungseinträge, in denen Anbieter über ihre eigenen Angebote sprechen. Die Beiträge der Studienpartner ab Seite 76 sind als solche gekennzeichnet und gehen in keine Auswertung ein. Aussagen über den Bestand beziehen alle 172 Lösungen ein.

Das Zielbild war Voraussetzung der Erhebung, kein Ergebnis. Gespräche und Befragung veränderten es an mehreren Stellen. Der folgende Abschnitt beschreibt die Grenzen der Aussagekraft.

ABLAUF

Ablauf der Studie



ERGEBNIS

Fünf Kernbefunde · Zielbild · 30 Maßnahmen

Stufe 1 und 2 gehen der Erhebung voraus. Interviews und Befragung laufen parallel und werden erst in Stufe 4 zusammengeführt.

Abb. A.1: Studienleitung GSÖ 2030

Grenzen der Aussagekraft

Diese Studie erhebt keinen Anspruch auf Repräsentativität. Sie zeigt, was Beteiligte aus ihrer Praxis berichten, und gleicht es gegen Daten ab. Wo das nicht trägt, steht es hier.

Das Sample ist nicht ausgewogen. Von 61 Gesprächspartnern kommen 20 aus Technologie und Verteidigungsindustrie. Das ist die Folge der Partnerstruktur dieser Studie und bedeutet, dass die Anbietersicht stärker vertreten ist als die kommunale Ebene. Drei Gesprächspartner werden auf eigenen Wunsch nicht genannt.

Der internationale Vergleich ist nicht extern geprüft. Der Peer-Review der Reifegrad-Matrix steht aus, Stand März 2026. Für zwei der zehn Dimensionen steht bewusst kein Wert, weil die Datenlage in allen Ländern zu dünn ist: Lage bewerten sowie Wiederherstellen und lernen.

Die Gewichtung entstand im Dialog. In drei Expertenworkshops haben die Studienpartner die Zwischenstände geprüft und geholfen, Wichtiges von Unwichtigem zu trennen. Das hat der Studie genützt und bedeutet zugleich: Welche Befunde Gewicht bekamen, folgt nicht allein aus den Daten. Auf Formulierung, Befunde und Maßnahmen hatten die Partner keinen Einfluss. Die Redaktion lag durchgehend bei der Studienleitung.

Nicht jede Lösung ist belegt. Von 131 in Gesprächen genannten Lösungen sind 16 durch einen Praxisbeleg gestützt, die übrigen beruhen auf Selbstauskunft oder auf der Nennung durch Dritte. Aussagen über Reife und Marktangebot stützen sich deshalb auf die 41 Einträge aus der Befragung, in denen ein Anbieter über sein eigenes Angebot spricht.

Bei Transkription, Codierung und Textredaktion kam KI-Unterstützung zum Einsatz, durchgehend das Sprachmodell Claude von Anthropic. Jede Zahl wurde gegen die Rohdaten nachgerechnet, jedes Zitat im Transkript geprüft, und zitiert wird ausschließlich aus Fassungen, die der Gesprächspartner freigegeben hat. Maschinelle Codiervorschläge wurden einzeln bestätigt. Die inhaltliche Verantwortung liegt bei der Studienleitung.

ABLAUF

Erhebungsinstrumente im Vergleich

Gesprächsleitfaden

55 Interviews · 60 Minuten · 22 Fragen

- 1 · Einstieg & Systemgrenze**
2 Fragen · Rolle und erlebte Grenze
- 2 · Use Case & Referenzlage**
2 Fragen · Szenario oder Erfahrung
- 3 · Wirkungsbrüche**
8 Fragen · die Bruchstellen sichtbar machen
- 4 · Rollen & Fähigkeiten**
4 Fragen · wer handelt, was fehlt ihm
- 5 · Hebel & Lernen**
3 Fragen · was wirkt, was andere gelernt haben
- 6 · Goldfrage**
1 Frage · offen am Ende
- 7 · Angebot & Rolle**
2 Fragen · nur Partnern gestellt

Online-Befragung

N = 72 · 8 Blöcke · rund 27 Fragen

- 1 · Einordnung**
3 Fragen · Rolle und Umfeld
- 2 · Ihre Lösung**
5 Fragen · Reifegrad, Dual-Use
- 3 · Referenz-Use-Case**
5 Fragen · vier Klick, ein Freitext
- 4 · Operative Wirkung**
3 Fragen · Beitrag und Evidenz
- 5 · Integrationsreife**
3 Fragen · Schlüsselmerkmale
- 6 · Bremsfaktoren**
3 Fragen · Zeithorizont, Top drei
- 7 · Hebel bis 2030**
1 Frage · Prioritäten
- 8 · Follow-up**
3 Fragen · Vertiefung und Kontakt

Beide Instrumente fragen dasselbe aus zwei Richtungen: Der Leitfaden beginnt bei der erlebten Systemgrenze, die Befragung bei der einzelnen Lösung.

Abb. A.1: Studienleitung GSÖ 2030

Glossar

Aufgenommen sind Begriffe und Abkürzungen, die im Text der Kapitel 1 bis 7 vorkommen. Die letzte Spalte nennt die Kapitel, in denen sie stehen.

Begriff	Auflösung	Kurzerklärung	Kap.
API	Application Programming Interface	Programmierschnittstelle; hier: standardisierter Datenabruf statt starrer Meldepflichten.	6
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	Bundesoberbehörde im BMI; höchstes Fachwissen im Zivilschutz, heute ohne operativen Durchgriff.	1, 4, 5, 7
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben	Betreibt Digitalfunk/BOS-Kernnetz; plant BOS-SIM-Karte und MC-Anwendungsplattform.	7
BG Klinik	Berufsgenossenschaftliche Klinik	Klinik der gesetzlichen Unfallversicherung, hier Ludwigshafen.	2, 5
BMI	Bundesministerium des Innern	Ressort mit Zuständigkeit für Bevölkerungs- und Zivilschutz.	1, 7
BOS	Behörden und Organisationen mit Sicherheitsaufgaben	Sammelbegriff: Polizei, Feuerwehr, Rettungsdienste, THW usw.	1, 5, 7
BSI	Bundesamt für Sicherheit in der Informationstechnik	Cyber-Sicherheitsbehörde des Bundes; zuständig u. a. für Zertifizierungen.	7
BWI	BWI GmbH (IT-Systemhaus des Bundes/Bundeswehr)	IT-Dienstleister der Bundeswehr.	1, 5, 6, 7
CBRN	chemisch, biologisch, radiologisch, nuklear	Sammelbegriff für Gefahrenlagen mit Kampfstoffen oder Strahlung.	1, 4, 7
Cell Broadcast		Flächige Warnung an Mobiltelefone ohne App, über die Funkzelle ausgelöst.	1
Cyber Nation Germany		BSI-DAX-40-Public-Private-Partnership, baut ein Cyber-Lagebild für Deutschland auf (Rindermann als Vorbild).	7
Delos Cloud		Souveräne Hyperscale-Plattform mit BSI-Zertifizierung für die öffentliche Verwaltung.	5
Delta		Ukrainisches Lage- und Tasking-System; Minimalstandard-Referenz (Delta-Basispackage).	3, 5
DKKV	Deutsches Komitee Katastrophenvorsorge	Fachnetzwerk für Katastrophenvorsorge.	2, 3, 7
D-LBO	Digitalisierung landbasierter Operationen	Programm der Bundeswehr zur Vernetzung der Landstreitkräfte.	1, 4
DRK	Deutsches Rotes Kreuz	Größte Hilfsorganisation.	1, 3, 5, 6, 7
EnBW	Energie Baden-Württemberg	Energieversorger und KRITIS-Betreiber.	4, 7
FEMA	Federal Emergency Management Agency	Katastrophenschutzbehörde der Vereinigten Staaten.	3, 5
Finnland		Schutzraumkultur, Selbstvorsorge als Bürgerpflicht; 1.300 km Grenze zu Russland.	3, 4, 6
FKIE	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie	Wehrtechnisches Forschungsinstitut (E = Ergonomie und Ethik).	1, 5, 6
Gesamtverteidigung		Zusammenspiel ziviler und militärischer Verteidigung als ein Planungsrahmen.	4
GMLZ	Gemeinsames Melde- und Lagezentrum von Bund und Ländern	Lagezentrum beim BBK ohne Weisungsbefugnis.	1, 4
GSM-R	Global System for Mobile Communications – Railway	Bahnfunkstandard, im Rückbau zugunsten FRMCS.	5
GSÖ	Gesamtstaatliches Sicherheitsökosystem	Leitkonzept der Studie: verteilte Fähigkeiten orchestrieren statt neue Strukturen bauen.	1, 2, 3, 4, 5, 6, 7
HiOrg	Hilfsorganisationen	Die fünf anerkannten: DRK, ASB, Johanniter, Malteser, DLRG.	1, 2, 6, 7
Host Nation Support		Unterstützung verlegender/durchreisender Bündnistruppen durch den Gaststaat; DE als Drehscheibe (Schaus, Hambach).	1, 4
IHK	Industrie- und Handelskammer	Regionale Vertretung der gewerblichen Wirtschaft.	4

Begriff	Auflösung	Kurzerklärung	Kap.
IMK	Innenministerkonferenz	Ständige Konferenz der Innenminister von Bund und Ländern.	1, 4
InnoZBw	Innovationszentrum der Bundeswehr	Innovationseinheit der Bundeswehr.	6
IRIS²	Infrastructure for Resilience, Interconnectivity and Security by Satellite	EU-Satellitenkonstellation für sichere, terrestrisch-redundante Kommunikation.	7
Katastrophen-schutzleuchttürme		Anlaufstellen (Schulen) mit WLAN und Strom im Krisenfall.	6
KLU	Kühne Logistics University	Private Hochschule mit Schwerpunkt Logistik und Lieferketten.	3, 4, 5, 6, 7
KRITIS	Kritische Infrastrukturen	Anlagen und Systeme mit essenzieller Bedeutung: Energie, Wasser, Kommunikation, Gesundheit, Logistik.	1, 4, 5, 6, 7
LCMS	Landelijk Crisis Management Systeem	Gemeinsame Lageplattform der niederländischen Sicherheitsregionen.	3, 5
LÜKEX	Länderübergreifende Krisenmanagement-Übung	Strategische Stabsrahmenübung von Bund und Ländern, seit 2004.	2, 7
MSDF	Multi-Sensor Data Fusion	Fusion von Sensordaten unterschiedlicher Träger zu einem einheitlichen Lagebild.	6
NATO	North Atlantic Treaty Organization	Nordatlantisches Bündnis; Referenz für Doktrin zu ziviler Resilienz und für Interoperabilitätsstandards.	1, 3, 5, 6, 7
NIS-2	Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau	EU-Richtlinie mit Melde- und Sicherheitspflichten für Betreiber wesentlicher Einrichtungen.	4
OODA-Loop	Observe – Orient – Decide – Act	Entscheidungszyklus; „Zeit geht beim Orient verloren“ – gemeinsame Lagebeurteilung nicht institutionalisiert. Rieks-Andockpunkt Kap. 7.	5
OpFüKdo	Operatives Führungskommando der Bundeswehr	Kommando für die nationale und territoriale Führung; Landeskommandos als regionale Ebene.	1
OPLAN DEU	Operationsplan Deutschland	~1.500-seitiger Bundeswehr-Plan für Landes-/Bündnisverteidigung im Inland; zivil fehlt ein Pendant.	4, 6
OT	Operational Technology	Betriebstechnik in Anlagen, abgegrenzt von der Informationstechnik.	5
Red Farmer Initiative		Rheinland-Pfalz: Landwirte registrieren freiwillig Assets (z. B. Güllewagen) für die Feuerwehr.	6, 7
Resilienz-API		Standardisierter gemeinsamer Andockpunkt, über den alle Systeme Daten interoperabel bereitstellen.	6
RessüLa	Ressortübergreifendes Lagebild (Name bezieht sich auf die Schnittstelle zu diesem Lagebild)	Technische Schnittstelle/Vernetzungsschicht, die zivile und militärische Lagedaten zwischen Datenbanksystemen medienbruchfrei überträgt und die Datenqualität erhält (Zweibahnstraße) – nicht das Lagebild selbst, sondern dessen Datenintegration. Vormalig TerrHub. Schaus (49) grenzt es ausdrücklich vom Lagebild ab; Hambach (48) nennt es verkürzt „ressortübergreifendes Lagebild“. Schreibweisen: Ressüla/RessüLa/RESSÜLA.	6
Rijkswaterstaat	niederländische Wasser-/Infrastrukturbehörde	staatliche Organisation mit weitreichenden Durchgriffsrechten (Deichbau, Flutung).	6
SAPIENT	– (Sensordaten-/Effektor-Schnittstelle)	Offene Schnittstelle für Sensor-/Effektor-Austausch; als Standard statt neuer Instanz.	6
SINA	Sichere Inter-Netzwerk-Architektur	Für Verschlusssachen zugelassene Kommunikationslösung.	6
STANAG 4676	NATO Standardization Agreement 4676	NATO-Standard für die Interoperabilität von Sensor- und Aufklärungsdaten.	6
Starlink		Kommerzielle Satellitenkommunikation; operativ stark, aber Souveränitätsrisiko (SpaceX).	5
TerrC2	Territoriales Führungssystem	Führungsstruktur der Bundeswehr im Inland.	4
THW	Technisches Hilfswerk	Bundesbehörde für technische Hilfe im Katastrophenschutz.	1, 2, 4, 7
Vigilanz		Wachsamkeit/Früherkennung vor der Krise; als Ergänzung/Gegenbegriff zu reiner Resilienz (Forschung vor der Krise).	3
ZOES	Zukunftsforum Öffentliche Sicherheit	Sicherheitspolitisches Forum.	7

Quellenverzeichnis

A · Eigene Erhebungsgrundlagen

Grundlage	Umfang	Stand
Interviewkorpus GSÖ 2030	55 Tiefeninterviews und zwei schriftliche Beiträge, 61 Gesprächspartner, davon 50 quantitativ ausgewertet	März bis August 2026
GSÖ-Befragung	Online-Befragung unter Technologieanbietern und Anwendern, N=72	Feldschluss 14.06.2026
Lösungs-Datenbank GSÖ 2030	172 Lösungen, davon 131 aus Interviews und 41 aus der Befragung	V14 · Juli 2026
Maßnahmen-Datenbank GSÖ 2030	529 Vorschläge	V3_4 · Juli 2026
Maßnahmen-Bewertung	162 bewertete Vorschläge mit Gate, Score und Track	V3_2 · Juli 2026
Beispieldatenbank GSÖ 2030	Dokumentierte Krisen- und Referenzfälle im In- und Ausland	V5 · Juli 2026
Benchmark Systemreifegrad	10 Dimensionen, 6 Länder	V2 · März 2026
GSÖ-Zielbild	Ebenen 1 bis 7, navigierbare Fassung	V5 · 2026
Auswertungsraster GSÖ 2030	Codierschema für Interviews und Befragung	3.1 · 2026
Meta-Research GSÖ 2030	Auswertung vorliegender Studien, Berichte und Rechtsgrundlagen	2026
Thesepapier Sicherheitsökosystem 2030	Executive Edition, Vorstudie	März 2026
Fallstudie Landkreis Neuwied	Eigene Erhebung	2026

B · Externe Quellen

Quelle	Jahr	Güte	Abschnitte
acatech-Studie Innovationssystem Deutschland	2026	wissenschaftlich	1.2, 4.7, 6.4
acatech-Studie · Dealroom · Bitkom DefTech Report	2026	wissenschaftlich	4.7
acatech-Studie · Deutscher Bundestag · Universität der Bundeswehr	2026	wissenschaftlich	7.4
acatech-Studie · Stifterverband	2026	wissenschaftlich	6.1
BAKS-Arbeitspapier Bedingt resilient	2026	amtlich	2.4, 4.3
BAKS-Arbeitspapier Behnke und Limbach, 17.02.2026	2026	amtlich	4.7
BBK · BAKS	2026	amtlich	2.5
BBK, Magazin Bevölkerungsschutz 1/2026	2026	amtlich	1.2
BBK, Ratgeber Vorsorgen für Krisen und Katastrophen	2026	amtlich	6.5
BBK, repräsentative Umfrage zum Bundesweiten Warntag	2026	amtlich	6.5
BBK, Themenseite Stromausfall	2026	amtlich	1.4
BBK-Erhebungen, referiert 2026	2026	amtlich	6.5
BCG Henderson Institute, Februar 2026	2026	Beraterstudie	4.7
BCG Henderson Institute, The Defense Technology Frontier, Februar 2026	2026	Beraterstudie	4.7
BCG und MSC, fünfte Ausgabe, 11.02.2026	2026	Beraterstudie	7.4
zitiert in BCG und MSC, MSC 2026	2026	Beraterstudie	7.4
BCG, Debunking the Five Myths Behind the Munitions Gap	2026	Beraterstudie	7.4
BCG, The New Frontier of Defense Technology and Security	2026	Beraterstudie	4.7
Bertelsmann Stiftung, Resilienz und Wirtschaftssicherheit	2025	wissenschaftlich	3.7
Bitkom, Wirtschaftsschutz 2025	2025	Verbandsstudie	2.4, 4.7
Bitkom, Wirtschaftsschutz 2025 (n=1.002 Unternehmen)	2025	Verbandsstudie	2.4
Bitkom, Wirtschaftsschutz-Reihe 2023 bis 2025	2025	Verbandsstudie	4.7

Quelle	Jahr	Güte	Abschnitte
Bitkom, zur it-sa 2025	2025	Verbandsstudie	4.7
BMFTR, Programm Forschung für die zivile Sicherheit	2026	amtlich	Epilog
BMI und Bundesregierung, Ehrenamt im Bevölkerungsschutz	2026	amtlich	1.2
BSI, Lagebericht zur IT-Sicherheit in Deutschland 2025	2025	amtlich	2.5
Bundesnetzagentur, SAIDI-Auswertung 2024	2024	amtlich	1.1
Bundeswehrbeschaffungsbeschleunigungsgesetz	2026	amtlich	7.4
Bundeszentrale für politische Bildung	2026	Schätzung / amtlich	1.1, 1.2
Bundeszentrale für politische Bildung, Akteure des Bevölkerungsschutzes	2026	wissenschaftlich	1.2
Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag	—	amtlich	1.1
Check Point Research	2026	Anbieterstudie	2.4
Civey im Auftrag von Deloitte, n=5.000	2026	Beraterstudie	1.1, 6.5
Europäische Kommission, COM(2026) 81	2026	amtlich	6.4
FEMA, National Preparedness Goal	2015	amtlich	3.3
Finnische Regierung, Security Strategy for Society	2025	amtlich	3.5
Gesellschaft für Sicherheitspolitik, Projekt Gesamtverteidigung	2026	amtlich	Epilog
HWWI, Value of Lost Load · TU Berlin	2013 und 2011	wissenschaftlich	2.4
ifo Institut	2024 und 2025	wissenschaftlich	1.2
ifo Institut, Kurzexpertise für das BMF	2024	wissenschaftlich	1.2
IfW Kiel, Kiel Report Nr. 2	2025	wissenschaftlich	4.7
Innenministerkonferenz, Bund-Länder-Arbeitsgruppe, 09.05.2025	2025	amtlich	1.4
NATO Defence Planning Process	2023	amtlich	3.4
NATO, Resilience and Civil Preparedness	2021	amtlich	3.2
PwC, Strategy& und DGAP, MSC 62	2026	Beraterstudie	3.5
Rat der EU, Digital Omnibus, Beschluss 29. Juni 2026	2026	amtlich	6.3
Schwedische Regierung	2026	amtlich	3.5
Strategy& und BAKS, MSC 2026	2026	Beraterstudie	4.7
Umweltbundesamt, Indikator BS-R-4	2021	amtlich	1.2
Umweltbundesamt, Monitoring zur Deutschen Anpassungsstrategie, Indikator BS-R-4	2024	amtlich	1.2
Universitäre Panelstudie zur Notfall- und Katastrophenvorsorge, Welle 3	2025	wissenschaftlich	6.5
Interview Vorstand Lasertechnik, F.A.Z.	2026	Anbieterstudie	2.6, 4.7, 7.1
ZöIS Spotlight 1/2026, Exzellenzcluster SCRIPTS	2026	wissenschaftlich	6.5

C · Rechtsgrundlagen

Norm	Fundstelle	Kap.
Grundgesetz	insbesondere Artikel 35 und 87a	1, 4
KRITIS-Dachgesetz		1, 4
Luftsicherheitsgesetz	insbesondere § 15a	4
Bundespolizeigesetz	Novelle vom 10. Juli 2026	4
NIS-2-Richtlinie und Umsetzung		4
Katastrophenschutzgesetze der Länder		2, 4
Sicherstellungs- und Vorsorgegesetze des Bundes		4
Bundeswehrbeschaffungsbeschleunigungsgesetz		7
Beschlüsse des Nationalen Sicherheitsrats	vom 8. Juni 2026	4