CIVITAS EUROPE

EIN UNTERNEHMEN DER VEKTOR GROUP

ANGRIFF AUF KRITISCHE INFRASTRUKTUR

Führungsfähigkeit unabdingbar für resiliente Reaktion

Hagen Peukert

WHITEPAPER · NOVEMBER 2026

03. November 2026

Herausgeber: CIVITAS Europe

Ein Unternehmen der Vektor Group · civitas-europe.de

1. KRITIS: Vulnerable Zahnräder einer offenen Gesellschaft

Weltweit steigen die erfassten Vorfälle, die die Störung, Lähmung oder Zerstörung bestehender Anlagen und Einrichtungen zum Ziel haben. Ob Cyberangriffe gegen öffentliche Einrichtungen, Behörden oder Unternehmen - vorgetragen von Kriminellen und/oder staatlichen Akteuren, die physische Zerstörung von Stromnetzen, die Behinderung und zeitweilige Lähmung von Verkehrsnetzen und -knotenpunkten, aber auch extern gesteuerte Sabotage[1], Desinformation und Manipulation - sie alle addieren zu den täglichen Gefahren und Risiken, die sich aus Unfällen, Schadensereignissen, Naturkatastrophen in einer hochindustrialisierten und global vernetzten Gesellschaft abspielen. Die Bitkom-Studie Wirtschaftsschutz 2025 beziffert den Gesamtschaden durch Diebstahl, Spionage und Sabotage auf 289,2 Mrd. Euro; davon entfallen 70 Prozent auf Cyberangriffe.[2] Die Folgen, die sich aus stark zersiedelten Großräumen, regulierten Naturräumen und den Bedingungen des Klimawandels in immer schnellerer Abfolge ereignen, fordern Resilienz und Krisenbewältigung deutlich heraus.

Neben den teilweise schweren Beeinträchtigungen durch Schließungen des täglichen Betriebs oder Beeinträchtigung der Mobilität ist der finanzielle Schaden enorm.

Der russische Krieg gegen die Ukraine zeigt, wie durch die Zerstörung kritischer Infrastruktur eine Gesellschaft und ein souveräner Staat militärisch besiegt oder von innen heraus destabilisiert werden sollen. Das Kalkül: Kritische Infrastruktur als Lebensnerv und die Basis für öffentliches und individuelles Leben wird entzogen.

Ob in Krieg und hybriden Szenarien, nach Katastrophen und Großschadensereignissen- der Schutz Kritischer Infrastruktur betrifft alle und ist eine gesamtgesellschaftliche Aufgabe.

Mit dem 2026 verabschiedeten KRITIS-Dachgesetz wurde ein rechtlicher Rahmen zur Stärkung der physischen Resilienz kritischer Anlagen geschaffen.[3] Welche Anlagen erfasst werden und wann einzelne Pflichten greifen, richtet sich nach dem Gesetz und seiner konkretisierenden Verordnung.[4] Den Betreibern kritischer Anlagen werden Maßnahmen auferlegt, die deren Resilienz stärken sollen. Dazu gehört die Erarbeitung und Umsetzung von Resilienzplänen, in denen auf der Basis von Risikoanalysen und -bewertungen der Betreiber dargestellt wird, welche geeigneten und verhältnismäßigen technischen, sicherheitsbezogenen und organisatorischen Maßnahmen zur Stärkung der Resilienz getroffen werden.[5]

Auf Behörden wie auf öffentliche und private Betreiber kommen Erfüllungsaufwand und Pflichten zu, deren konkrete Ausgestaltung vom jeweils geltenden Rechtsrahmen abhängt. Damit verbundene Datenerhebungen sind ihrerseits schutzbedürftig.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) übernimmt Aufgaben im Rahmen des KRITIS-Dachgesetzes, unter anderem bei der Registrierung kritischer Anlagen. Neben dem physischen Schutz gewinnen damit der laufend aktualisierte Grunddatenbestand und die analytische Auswertung von Überprüfungen und Schwachstellen an Bedeutung.

BBK und Bundesamt für Sicherheit in der Informationstechnik (BSI) übernehmen Aufgaben in ihren jeweiligen gesetzlichen Zuständigkeitsbereichen. Die operative Führung im Katastrophenschutz richtet sich nach dem Landesrecht und den Zuständigkeiten vor Ort.

Gleichwohl: Die föderale Gliederung und nachfolgende Struktur der Bundesrepublik sieht in der Reaktion auf Großschadensereignisse und Katastrophen eine Vielzahl von ebenengebundenen und -übergreifenden Kompetenzen und Akteuren aus dem behördlichen und nicht-behördlichen Bereich vor. Die Verfahren zur Zusammenarbeit, Verantwortungsübernahme und einem gemeinsamen Management sind zwar teilweise formell geregelt, unterliegen in der Praxis mit ihren stets aufs Neue zu erfassenden Führungsorganisationen, Kompetenzen und Bewältigungsmaßnahmen jedoch immer wieder notwendigem Ad-hoc-Anpassungsdruck, der vor allem Zeit kostet.

Nicht selten behindern Verantwortungsdiffusion, Ressourcendenken und andere Rücksichtnahmen die Aufnahme, Einleitung und Bewältigung umfassend koordinierter Maßnahmen. Der Abschlussbericht zur sogenannten “Ahrtalkatastrophe”[6], aber auch die Erkenntnisse aus der COVID-19-Pandemie verdeutlichen nicht nur die Mängel, sondern vor allem die immensen Herausforderungen, denen sich Führung und Entscheidungsträger ausgesetzt sehen, vor allem in multiplen, vielschichtigen Ereignissen mit sekundären und Folgewirkungen, in paralleler und/oder zeitversetzter Abfolge auf Basis vorhandener, möglicherweise aber unzureichend bereitgestellter Informationen richtige und schnelle Entscheidungen zu treffen.

Nachfolgende Abbildung[7] mag am Beispiel der Cybersicherheitsarchitektur in Deutschland genügen, um die augenscheinliche Vielschichtigkeit und Komplexität verantwortlicher Behörden und Akteure zu illustrieren. Die Vielzahl beteiligter Stellen erhöht den Abstimmungsbedarf bei der Erstellung eines gemeinsamen Lagebildes. Zwangsläufig stellt sich die Frage, - wer - wann und - womit darauf zu reagieren hat bzw. wem eine Führungsrolle dabei zukommt. Im Katastrophenfall und nach Großschadensereignissen kommen ähnliche Koordinierungsaufgaben auf alle Beteiligten zu. Bei der Beantwortung und Klärung dieser Sachverhalte vergeht wertvolle Zeit, werden unter Umständen wesentliche Informationen übersehen und somit richtige Entscheidungen erschwert.

Cybersicherheitsarchitektur

Gesamtübersicht · vergrößerte Detailansichten auf den Seiten 11–16

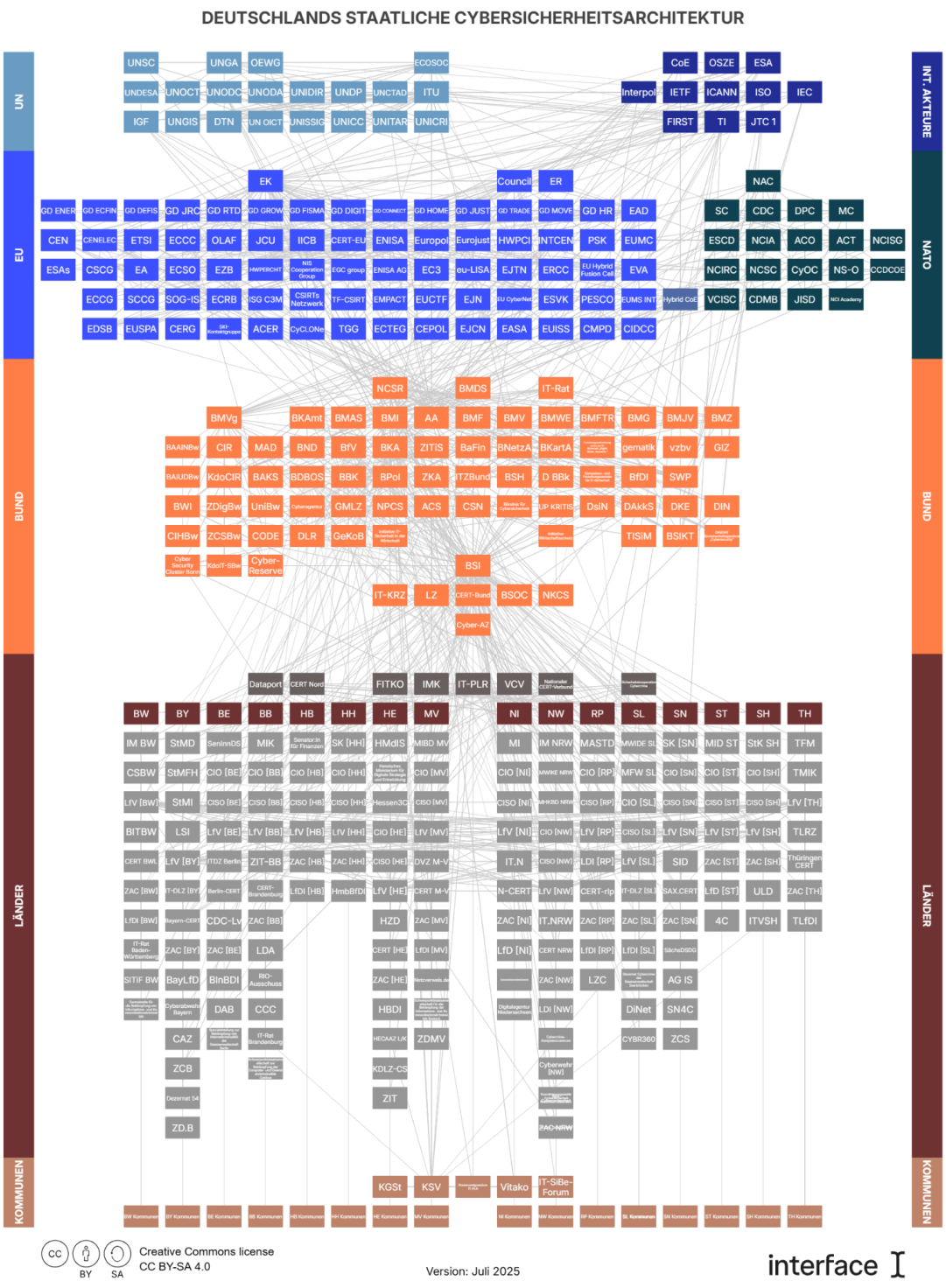


Abbildung 1 · interface · Version Juli 2025 · CC BY-SA 4.0.

Die Übersicht zeigt die Vernetzung. Einzelne Einträge bitte im Anhang lesen.

Interaktive Quelle: cybersicherheitsarchitektur.de

Spätestens seit 2022 hat sich in Europa die Sicherheitslage grundlegend verändert. Resilienz kritischer Infrastruktur wird nun auch in militärischer Hinsicht mitbedacht und in die militärische Verteidigungsplanung miteinbezogen. Auch angesichts physischer Bedrohung und Zerstörung müssen Staat und Gesellschaft funktionieren, standhalten und sich ihre Existenz bewahren können. Der Operationsplan Deutschland berücksichtigt auch den Schutz verteidigungswichtiger Infrastruktur.[8] Der Zusammenhang mit dem KRITIS-Dachgesetz ist im jeweiligen Aufgaben- und Rechtsrahmen zu betrachten.

2. Gut vorbereitet auf komplexe und dynamische Lagen?

Auch ohne offene kriegerische Handlungen stellen multiple Großschadensereignisse, ggf. aber unter hybriden Ursachen und parallelen oder sukzessiven Folgeereignissen und -effekten vor allem das entscheidungsbefugte Stabs- und Führungspersonal vor große Herausforderungen und Belastungen. Ein fiktives Beispiel:

Die nachfolgenden Zahlen und Ereignisse sind fiktive Szenarioannahmen, keine Prognose oder Bewertung der tatsächlichen Sicherheit des Standorts. In einem fiktiven Szenario, dem der BASF-Standort Ludwigshafen zugrunde liegt, wird ein chemieverarbeitendes Produktionsareal mit etwa 35.000 Beschäftigten angenommen. Dort kommt es zu mehreren Explosionen, die zu großen Opferzahlen (mehr als 7.000) führen und eine hochgiftige Pollution freisetzen, die wiederum die Evakuierung von mehr als 250.000 Bewohnern aus einem festzulegenden Ballungsraum erfordert, die Schließung der Binnenschifffahrt und Sperrung des Luftraumes erzwingt. Eine stabile Inversionswetterlage führt zu keinem wesentlichen Luftaustausch; der Aufenthalt für Bewohner und Rettungskräfte ist gesundheitsgefährdend. Strom- und Energieversorgung müssen zeitweise bzw. dauerhaft erheblich eingeschränkt werden. Evakuierung, Versorgungsknappheit und polizeiliche Maßnahmen führen stellenweise zu sozialen Konflikten, die wiederum zu Desinformationskampagnen in den Sozialen Medien (Deepfakes, Falschinformationen) führen. Die tagelange Schließung von Verkehrswegen stört Lieferketten; es kommt zu Produktionsausfällen außerhalb des Katastrophengebietes. Hinweise auf Drohnenüberflüge und Sabotage führen zu einer Ausdehnung der Ermittlungen…

Vor diesem nur unvollständig skizzierten Szenario stellt sich allen Beteiligten und Experten die alles entscheidende Frage, wie unter größtem Zeit- und Handlungsdruck, bei graduell zunehmender physischer Erschöpfung und psychischer Dauerbelastung aus der Vielzahl von Meldungen, Hinweisen, Widersprüchen, Unklarheiten, Daten aus unterschiedlichen, oftmals nicht verifizierten Quellen, Kommunikationsfehlern, Annahmen und Hypothesen aus den Stäben, Optionen und Erwartungen einer ungeduldigen, mitunter kritischen Öffentlichkeit ein einziger oder vermutlich mehrere Führungs- und Einsatzstäbe richtige Entscheidungen treffen sollen. Wie kann man eine zunehmend komplexer werdende Ablauforganisation im Krisenmodus führen und koordinieren?

Was also benötigen Einsatzstäbe und Krisenmanager?

Das der Bundesregierung 2023 vorgelegte Grünbuch schreibt:

> *Vor dem Hintergrund bisheriger Erfahrungen und in Anbetracht künftiger Herausforderungen ist als Grundlage für Führung und Krisenmanagement die Entwicklung eines Interdisziplinären Lagebildes in Echtzeit rund um die Uhr für Deutschland unter Nutzung zukunftsweisender Technologien überfällig.*[9]

- Mit der Umsetzung des KRITIS-Dachgesetzes ist zusätzliches relevantes Datenaufkommen zu erwarten. Strukturierte Grund- sowie aktualisierte Messdaten und regelmäßige Bewertungen und Analysen schaffen die Grundlage für ein gemeinsames Lageverständnis.
- Im Krisen- und (Groß-)Ereignisfall wird sich das Lage- und Informationsbild auf diese Grunddaten verlassen und sich dann vermehrt auf aktuelle Lagedaten abstützen, die in unterschiedlicher Qualität, aus einer Vielzahl von Quellen und Sensoren in unterschiedlicher Geschwindigkeit generiert werden. Bislang in der Regel analog und mit menschlichen “Drehstuhlfunktionen” für die Auswertung und Koordinierung.
- Friktionen entstehen immer noch regelmäßig durch Ressourcen- und Silo-Denken, das zwar die Bedeutsamkeit der eigenen Organisation berücksichtigen und hervorheben mag, aber den effizienten Aufbau eines vollständigen, lagegerechten Ein- und Überblicks behindert. Der ebenenübergreifende Datenschutz kann in bestimmten Fällen zu Informationsverzug oder gar -abriss führen.
- Einsatzstäbe werden oft ad hoc gebildet. Qualifikation und Erfahrung im Umgang mit widersprüchlichen, unvollständigen und übersehenen Informationen variieren, bestimmen aber die Qualität von Führungsentscheidungen und -maßnahmen. Stäbe ermüden, brauchen Ruhezeiten. Viele Helfer unterliegen einer Rotation und stehen in einem Ehrenamt; ihre für die Aufgabe relevante Professionalität mag schwanken.
- THW, Freiwillige Feuerwehren, das DRK und verwandte Organisationen wie die Johanniter, die Malteser oder der Arbeiter-Samariter-Bund stützen sich wesentlich auf ehrenamtliches Personal. Mehrfachrollen können im Ernstfall zu konkurrierenden Verpflichtungen führen. Es besteht folglich Klärungsbedarf darüber, wer verbindlich und entsprechend ausgebildet für lagebearbeitende Funktionen und Führung zur Verfügung steht. Dies erschwert eine rasche und wirkungsvolle Reaktions- und Handlungsfähigkeit.
- Die Erfassung entsprechender Mitgliedschaften und Fähigkeiten setzt eine tragfähige Rechtsgrundlage und die Einhaltung der Datenschutzanforderungen voraus.[10]

Es sei nur am Rande erwähnt: Auch Unternehmen außerhalb des Anwendungsbereichs des KRITIS-Dachgesetzes stehen vor vergleichbaren Resilienzanforderungen. Je nach Tätigkeit und anwendbarem Rechtsrahmen treffen sie zudem weitere gesetzliche Verpflichtungen. Für sie erwachsen angesichts möglicher Szenarien Herausforderungen, die regelmäßig sehr schnell die existenzielle Überlebensfähigkeit infrage stellen.

Über die gesetzlich vorgesehenen Verwendungszwecke hinaus stellt sich die Frage, wie rechtmäßig verfügbare Daten für ein gemeinsames operatives Lagebild nutzbar gemacht werden können. Es bedarf also unter anderem einer definierten, eingeübten, ausgestatteten und professionellen Führungsorganisation. Natürlich gibt es dazu mehrere Optionen, die föderalen, geographischen, inhaltlich-organisatorischen und nicht zuletzt finanziellen Bedingungen und Vorgaben unterliegen.

3. Damit schlechtes Krisenmanagement zu keiner Staatskrise führt - gegen Kontrollverlust

Führungsfähigkeit in einer multiplen, komplexen und mitunter elementaren Krise und Katastrophe oder gar im Kriege ist unabdingbar und von essenzieller Bedeutung - über das Ereignis weit hinaus wirkend.[11]

Schlechtes Krisenmanagement, das auf unzutreffenden, verspäteten und unvollständigen (Teil-)Informationen beruht, wirkt sich nicht nur auf das aktuelle und konkrete Handeln aus, sondern führt in zunehmendem Maße zu politischen Folgereaktionen und gesellschaftlicher Frustration. Bürger und Bürgerinnen eines hochentwickelten Industrielandes erwarten von ihren demokratisch gewählten Amtsträgern (= sehr oft die Leiter von Krisen- und Katastropheneinsatzstäben) Reaktions- und Handlungsvermögen, gutes Krisenmanagement.

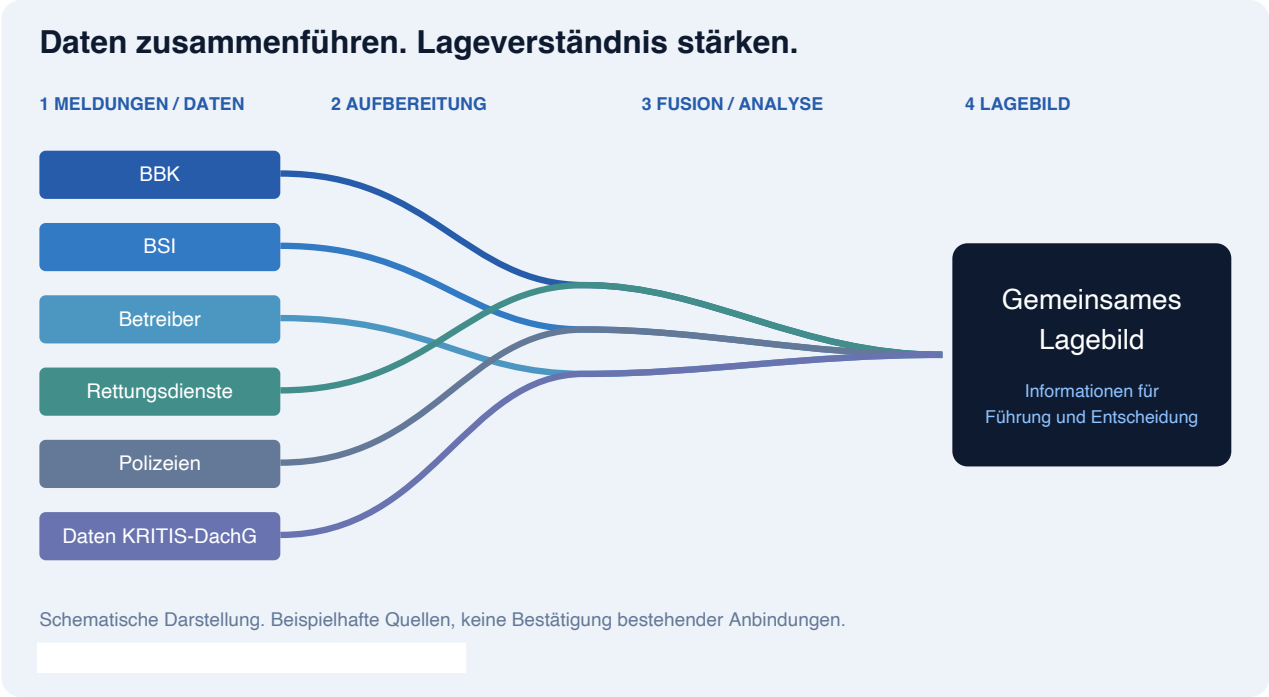
Wo dies fehlt, droht Vertrauensverlust, der sich bei vielen Bürgern in Staatsverdrossenheit und Abwendung erodierend auswirken kann. Der Staat und seine Organe müssen und - können - dafür sorgen, dass sich die angegriffene Resilienz kritischer Infrastruktur und Sicherung elementarer Lebensbereiche nicht zu einer Krise des Staates und seiner Strukturen auswächst.

Es geht also um einen neuen Fähigkeitserwerb und -zuwachs für politische Verantwortung und staatliche Organe, um in Katastrophen, Krisen und Krieg rasch, richtig und umfassend reagieren zu können.

4. Moderne Technologie stärkt Resilienz und Krisenbewältigung

Die gute Nachricht ist aber, dass mit überschaubarem, gleichwohl umfassendem und koordiniertem Ansatz eine technologische Lösung für die aufgezeigten funktionalen Defizite und Forderungen möglich ist, die zudem den Erfordernissen einer weitgehenden Datensouveränität und -hoheit Rechnung trägt.

- Moderne und vor allem verfügbare Informations- und Datenverarbeitung fusioniert vorhandene, oftmals strukturierte Grunddaten (wie zukünftig generiert gem. KRITIS-DachG) mit aktuellen Lage- und Messdaten, die sich aus einer Vielzahl verschiedener Akteure, Sensoren, Daten, Beschreibungen, Analysen und Aussagen zu einem einheitlichen, vielschichtigen und jederzeit nachvollziehbaren Gesamtlagebild zusammensetzen.
- Open-Source-Informationen (OSINT) kommt dabei eine neue, wesentliche Bedeutung zu. Nachrichten, Bilder, Anweisungen - sie alle können umfassend ausgewertet und einheitlich bearbeitet werden, und zwar in hoher Geschwindigkeit. Dies ist in einer Gesellschaft, wo nahezu jeder über mobile Endgeräte verfügt, eine nicht zu unterschätzende Informationsquelle.
- Künstliche Intelligenz hilft dabei, große Datenmengen zu strukturieren, bestehende Anwendungen nutzbar zu machen und miteinander zu fusionieren. Modular aufgebaut, werden alle identifizierten Ebenen vertikal und horizontal mit erforderlichen Informationen versorgt.
- Lagezentren und Entscheider können laufend aktualisierte Lageinformationen erhalten. Aktualität, Qualität und Verfügbarkeit hängen von Datenquellen, Berechtigungen und Betriebsbedingungen ab. Automatisierte, integrierte und variable Analyseanwendungen können so eine verzögerungsarme Entscheidungsfindung und Führungsfähigkeit unterstützen.



Schematische Darstellung zur Datenverarbeitung und -fusion aus unterschiedlichem Melde- und Beitragsaufkommen in offener und skalierbarer Architektur. Die dargestellten Stellen und Datenbestände sind beispielhafte Quellen; die Grafik weist keine bestehenden technischen Anbindungen aus.

- Dabei werden personelle Ressourcen geschont. Herkömmliche Drehstuhl-Schnittstellen - oftmals von Freiwilligen guten Willens und in unterschiedlicher Qualifikation besetzt - können reduziert werden oder erhalten nun Zugang zu zuverlässigen, redundanten und aktuellen Nachrichten und prozessierten Informationen. Entscheidungen gründen nun auf einer bislang nicht verfügbar zu machenden Vielfalt von Information in standardisierter Qualität und prononcierten Handlungsempfehlungen, die auf Kräfte, Raum und Zeit sowie vor allem auf Visualisierung und die Analyse von Bedrohungs- und Einflussfaktoren aufgebaut sind. Die Beurteilung von Worst-Case-Szenarien kann nun datengestützt vorgenommen werden.
- Der modulare Aufbau und die offene Architektur erlauben, eine Vielzahl von Akteuren und zuständigen Stellen ebenenunabhängig bzw. -übergreifend ein- und anzubinden. Entscheidungs- und Handlungssicherheit profitieren auf allen Ebenen von dem Zugang zu bzw. von der grundsätzlichen Verfügbarkeit relevanter Informationen. Ein tiefes und breites Lageverständnis trägt folglich dazu bei, richtig zu entscheiden und schneller zu handeln - vor Ort, in den Einsatzstäben, in Entscheidungszentren.
- In Vorbereitung und Unterstützung präventiver Maßnahmen können Szenarien und Lagen mit “echten” Daten simuliert werden - alle Ebenen profitieren durch Tiefenverständnis und verbesserte Vorbereitung.

Zukünftiges Krisenreaktionsvermögen, das die Wiederherstellung und den Erhalt kritischer Infrastruktur und öffentlicher Lebensbereiche zum Ziel hat, benötigt überlegene Führungsfähigkeit. In militärischem Kontext längst verfügbar, ist die Nutzung moderner Informations- und Datenfusion in komplexen und hybriden, in rascher Folge ablaufenden Krisen- und Katastrophenszenarien nicht mehr wegzudenken.

Und sie ist verfügbar. In Deutschland, für dessen Schutz und seinen Erhalt.

Quellen und Endnoten

1. Laut IISS stieg die Zahl bestätigter russischer Sabotageakte gegen Europas kritische Infrastruktur von 2023 auf 2024 um 246 Prozent. Charlie Edwards / Nate Seidenstein: The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure, August 2025, S. 9. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf

2. Bitkom: Wirtschaftsschutz 2025, Zusammenfassung. https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf

3. https://www.bundestag.de/dokumente/textarchiv/2026/kw05-de-kritische-infrastruktur-1137002

4. BBK: FAQ zum KRITIS-Dachgesetz, abgerufen am 03.11.2026. https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Strategien-und-rechtlicher-Rahmen/KRITISDachG/FAQ/faq_node.html

5. https://www.bundestag.de/dokumente/textarchiv/2026/kw05-de-kritische-infrastruktur-1137002

6. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2022/abschlussbericht-hochwasserkatastrophe.pdf?__blob=publicationFile&v=1

7. interface: Deutschlands staatliche Cybersicherheitsarchitektur, Version Juli 2025. Originalgrafik unter CC BY-SA 4.0; vergrößerte Ausschnitte im Anhang. https://www.cybersicherheitsarchitektur.de/ · Lizenz: https://creativecommons.org/licenses/by-sa/4.0/

8. https://www.bundeswehr.de/de/organisation/operatives-fuehrungskommando-der-bundeswehr/auftrag-und-aufgaben/operationsplan-deutschland

9. Zukunftsforum Öffentliche Sicherheit: aus Grünbuch; das Interdisziplinäres Lagebild in Echtzeit vom März 2023

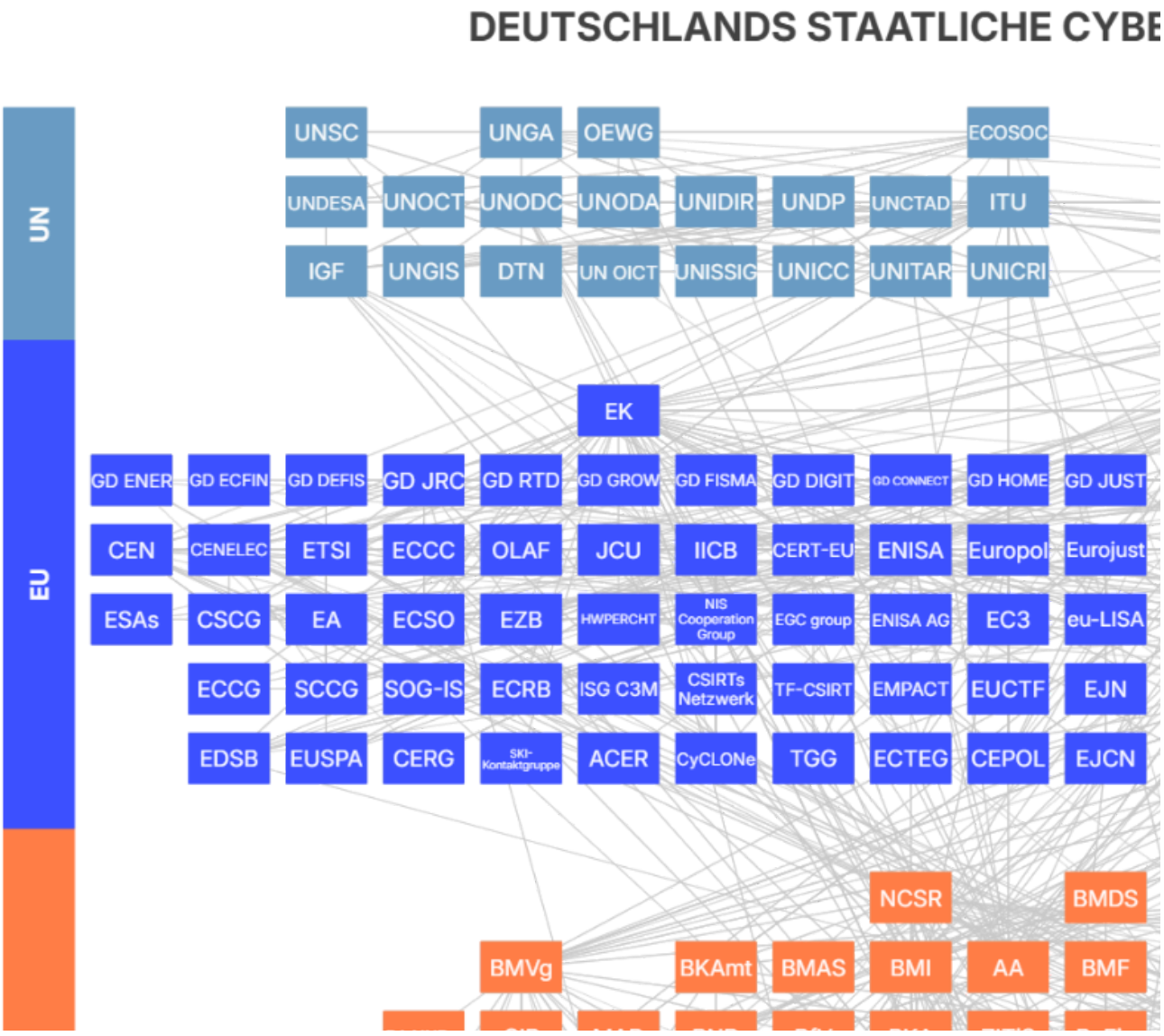
10. § 26 Bundesdatenschutzgesetz: https://www.gesetze-im-internet.de/bdsg_2018/__26.html · Zur Problematik von Mehrfachrollen: Julia Egleder, Bereit für den Ernstfall?, loyal, 02.02.2026. https://www.reservistenverband.de/magazin-loyal/gesamtverteidigung/

11. Vgl. Grünbuch. Interdisziplinäres Lagebild von 2023

Abbildung 1 · Detail 1 von 6

Oberer Bereich · linke Hälfte

Unveränderter Ausschnitt der Originalgrafik; benachbarte Bereiche überlappen.



Position in der Gesamtübersicht

1	2
3	4
5	6

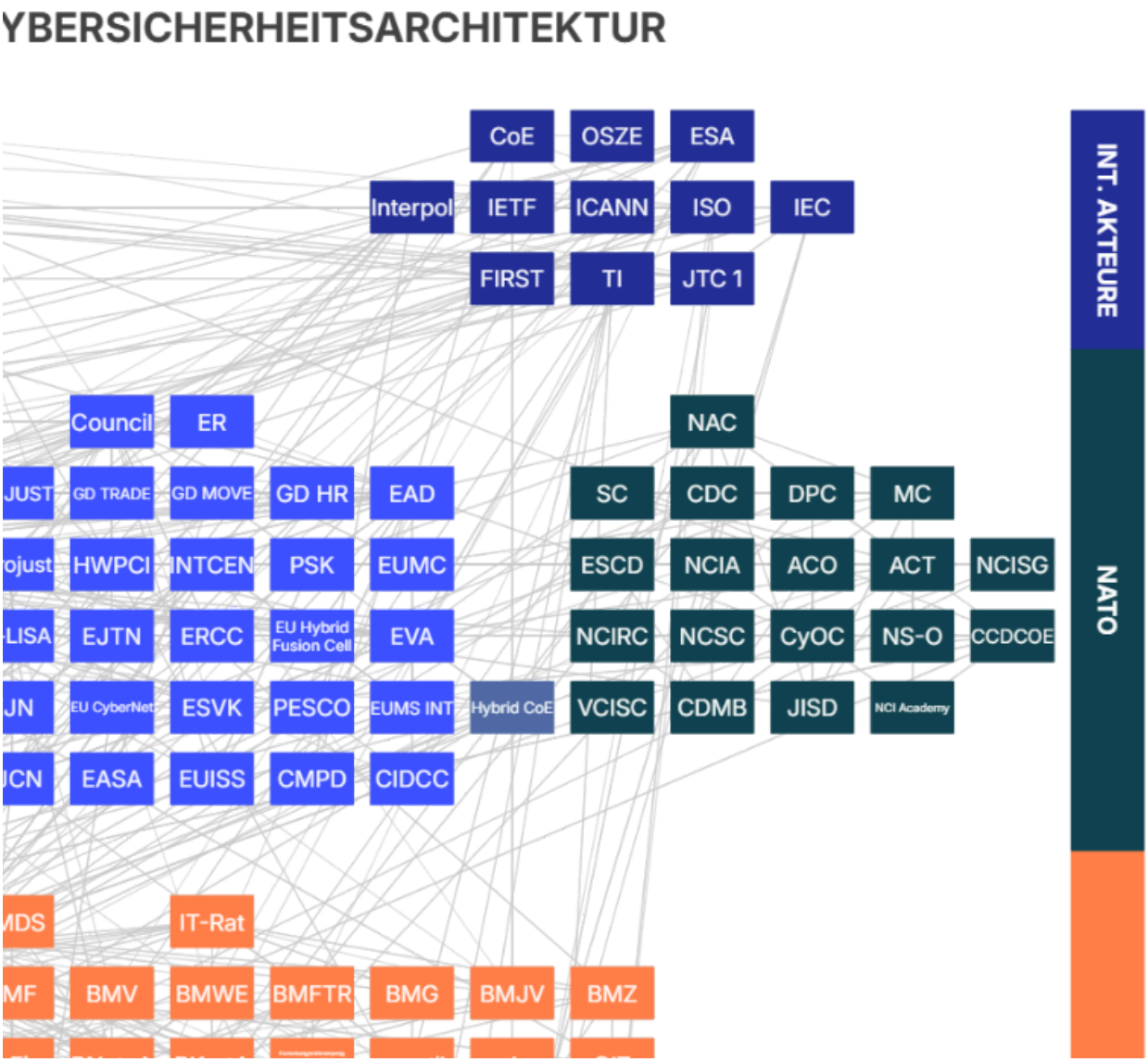
Zurück zur Übersicht: Seite 4

Quelle: interface · cybersicherheitsarchitektur.de · Originalstand des Whitepapers

Abbildung 1 · Detail 2 von 6

Oberer Bereich · rechte Hälfte

Unveränderter Ausschnitt der Originalgrafik; benachbarte Bereiche überlappen.



Position in der Gesamtübersicht

1	2
3	4
5	6

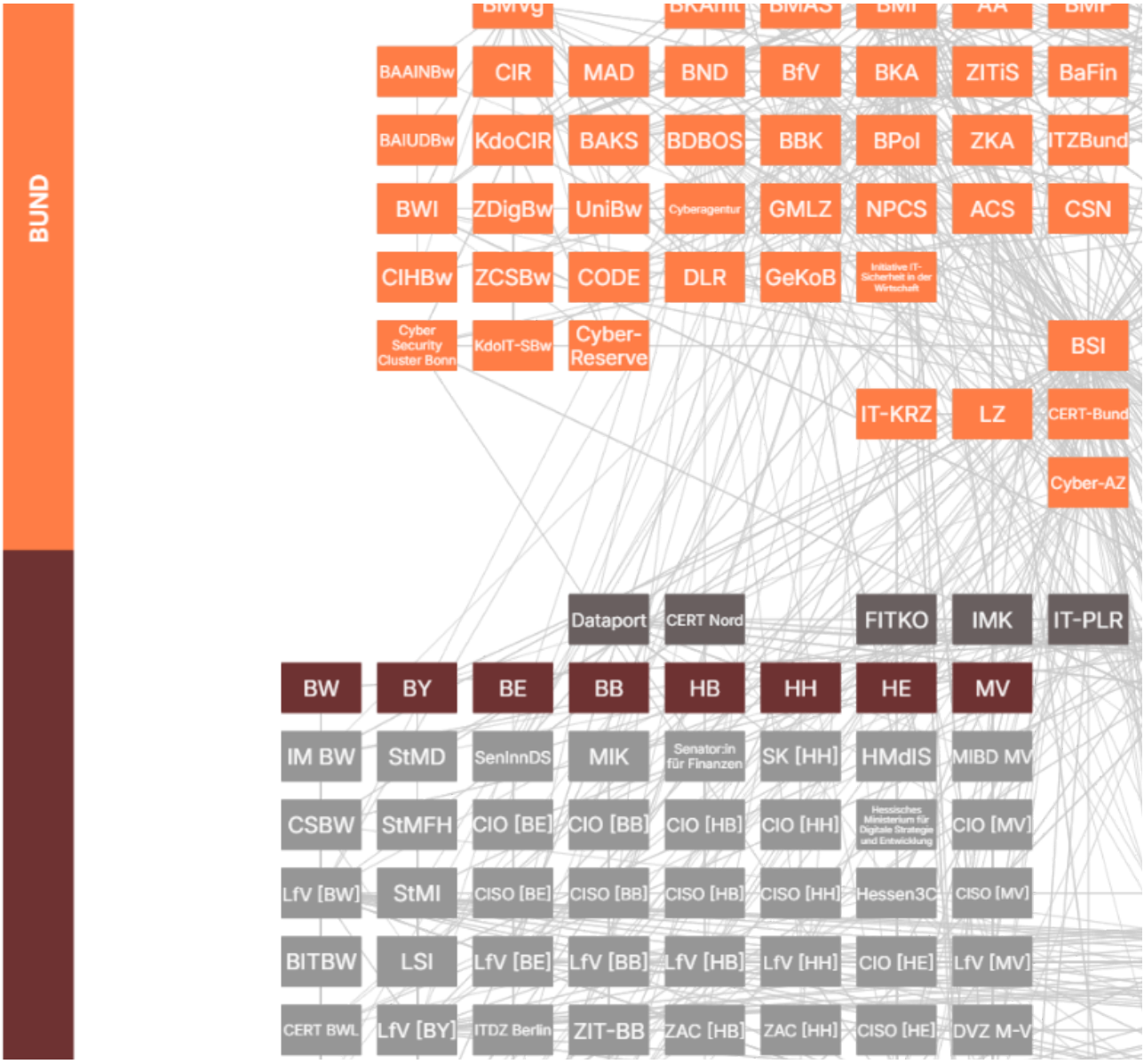
Zurück zur Übersicht: Seite 4

Quelle: interface · cybersicherheitsarchitektur.de · Originalstand des Whitepapers

Abbildung 1 · Detail 3 von 6

Mittlerer Bereich · linke Hälfte

Unveränderter Ausschnitt der Originalgrafik; benachbarte Bereiche überlappen.



Position in der Gesamtübersicht

1	2
3	4
5	6

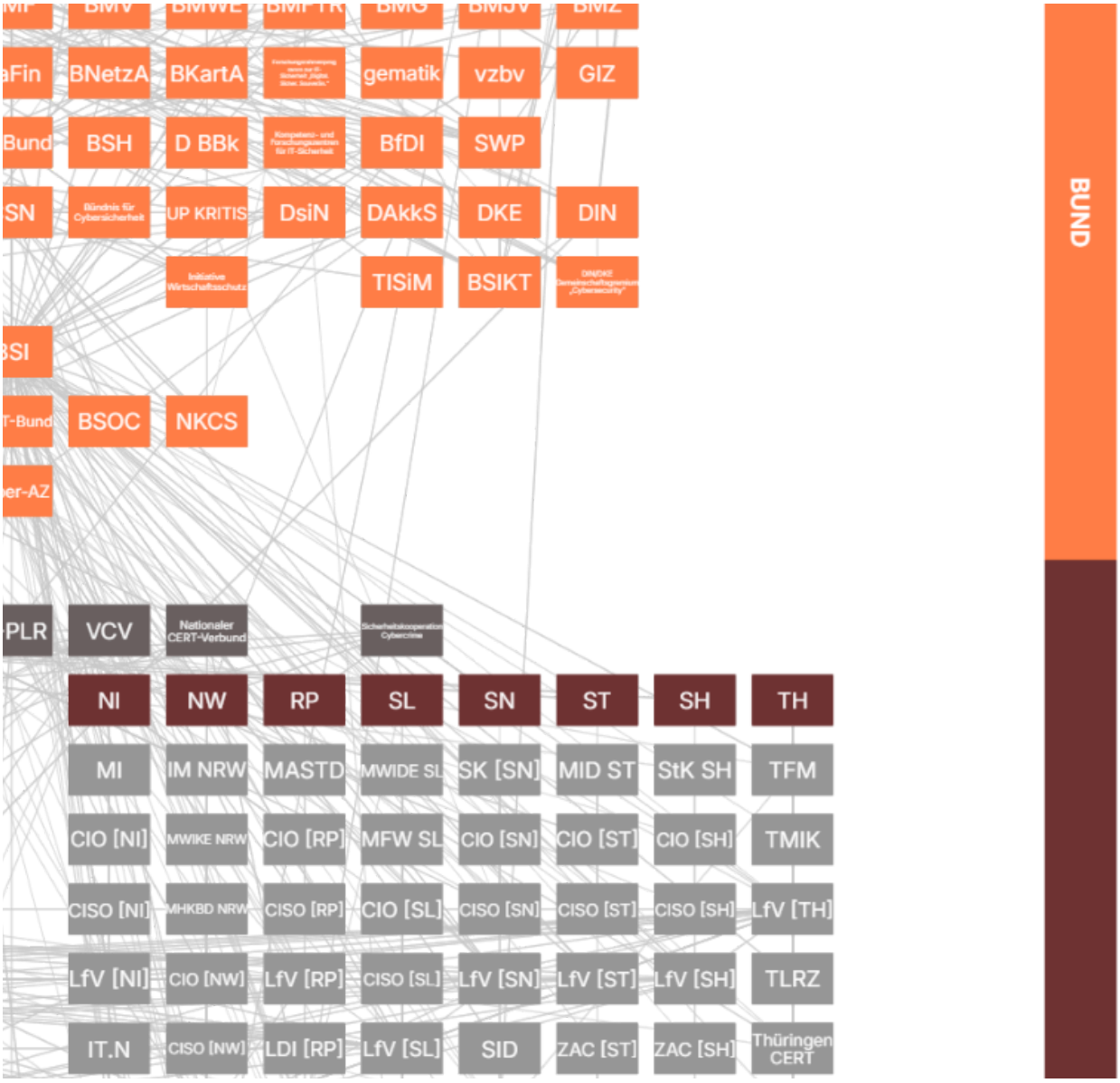
Zurück zur Übersicht: Seite 4

Quelle: interface · cybersicherheitsarchitektur.de · Originalstand des Whitepapers

Abbildung 1 · Detail 4 von 6

Mittlerer Bereich · rechte Hälfte

Unveränderter Ausschnitt der Originalgrafik; benachbarte Bereiche überlappen.



Position in der Gesamtübersicht

1	2
3	4
5	6

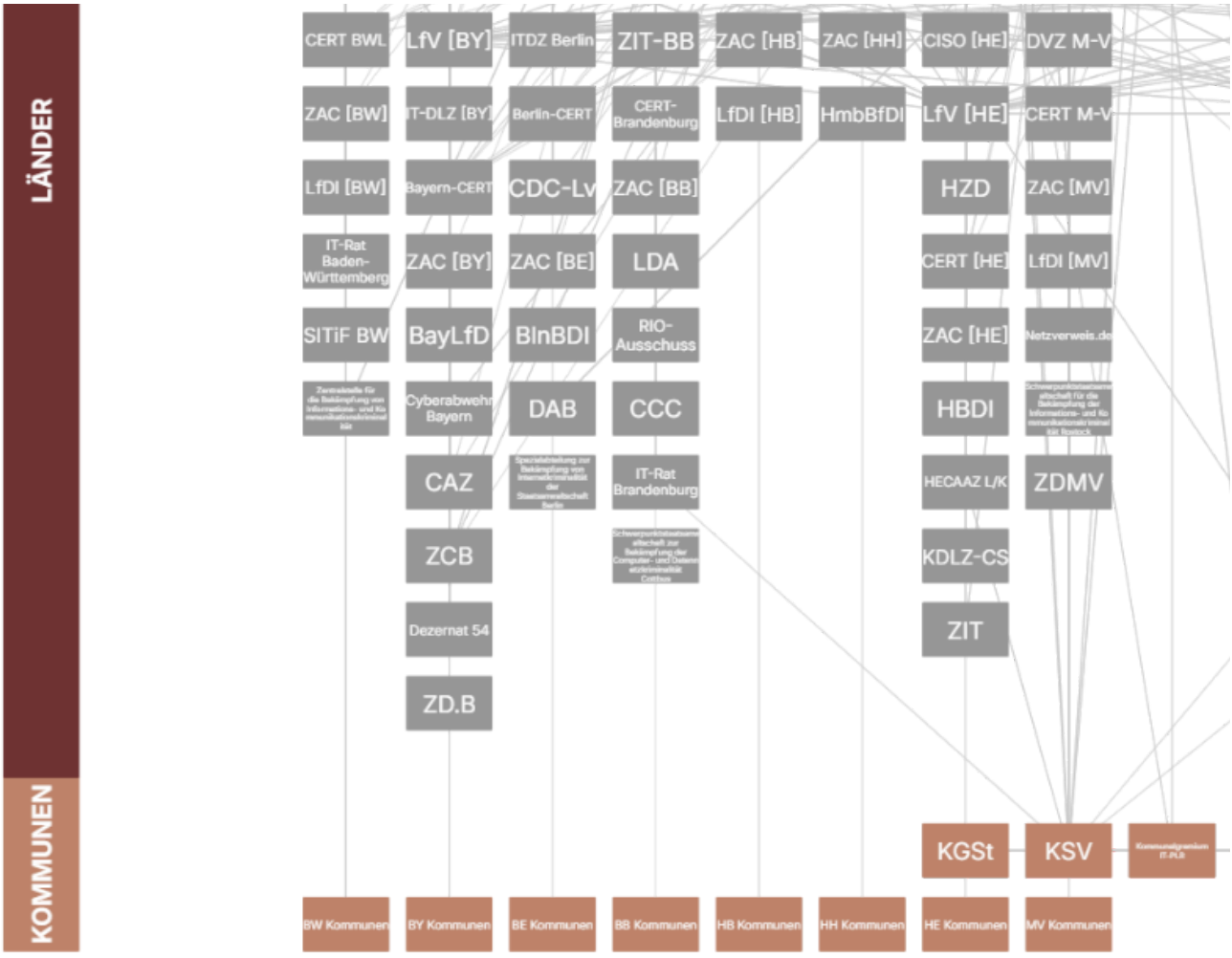
Zurück zur Übersicht: Seite 4

Quelle: interface · cybersicherheitsarchitektur.de · Originalstand des Whitepapers

Abbildung 1 · Detail 5 von 6

Unterer Bereich · linke Hälfte

Unveränderter Ausschnitt der Originalgrafik; benachbarte Bereiche überlappen.



CC BY SA
Creative Commons license
CC BY-SA 4.0

Version: Juli 2

Position in der Gesamtübersicht

1	2
3	4
5	6

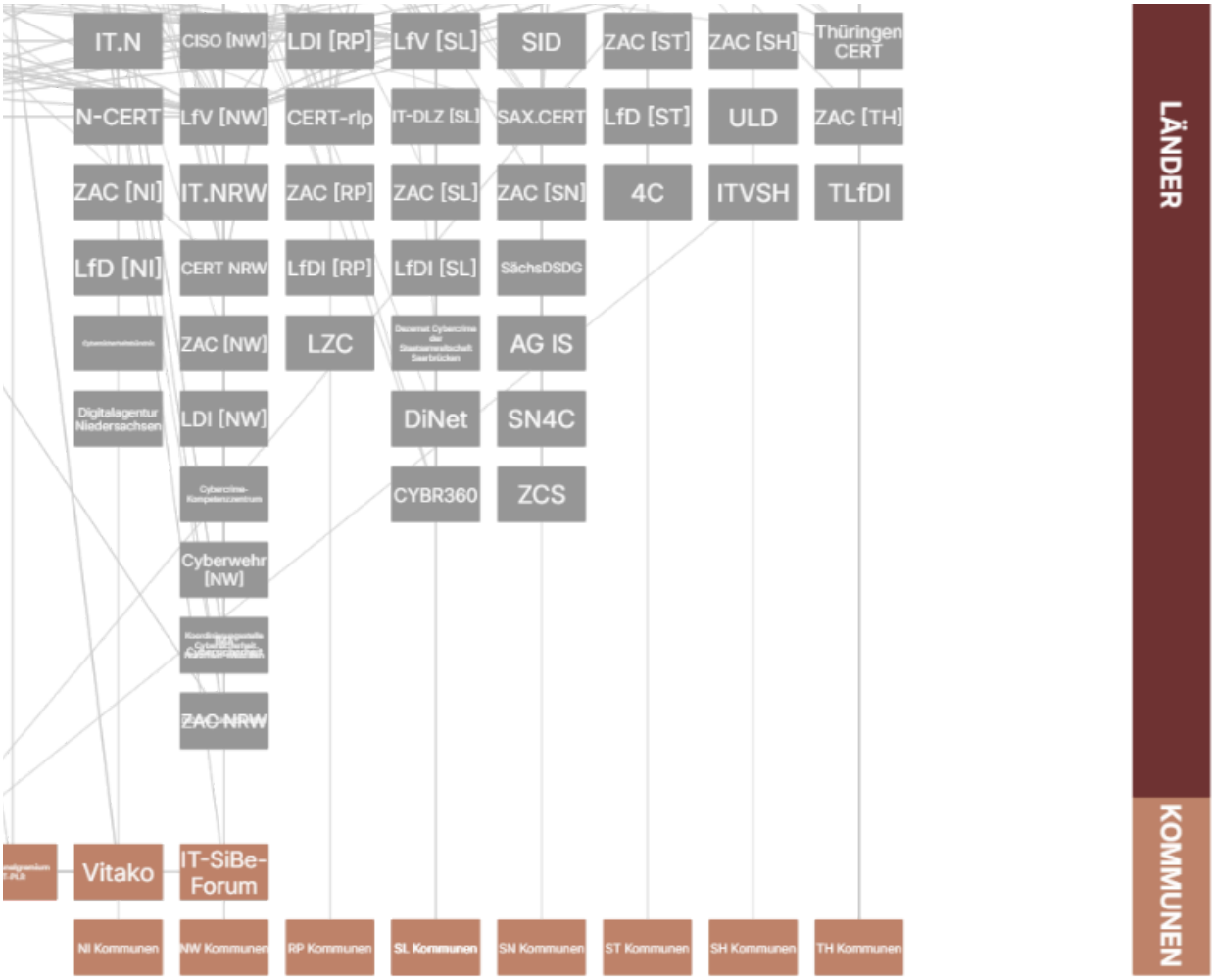
Zurück zur Übersicht: Seite 4

Quelle: interface · cybersicherheitsarchitektur.de · Originalstand des Whitepapers

Abbildung 1 · Detail 6 von 6

Unterer Bereich · rechte Hälfte

Unveränderter Ausschnitt der Originalgrafik; benachbarte Bereiche überlappen.



Juli 2025

interface

Position in der Gesamtübersicht

1	2
3	4
5	6

Zurück zur Übersicht: Seite 4

Quelle: interface · cybersicherheitsarchitektur.de · Originalstand des Whitepapers