

Digital resilient: Wie sich Deutschland krisenfest aufstellen kann

bitkom

Digital resilient: Wie sich Deutschland krisenfest aufstellen kann

Deutschland befindet sich in einer neuen sicherheitspolitischen Realität. Cyberangriffe, Sabotageakte und Desinformationen nehmen zu und treffen Staat, Infrastrukturen, Wirtschaft und Gesellschaft gleichermaßen. Hybride Angriffe zielen dabei nicht allein auf technische Systeme oder konkreten, materiellen Schaden. Sie zielen auch auf das Vertrauen in die Handlungs- und Verteidigungsfähigkeit des Staates.

Deutschland muss sich strategisch, praktisch und mental auf Krisenszenarien vorbereiten, die die digitale Infrastruktur, öffentliche Verwaltung, Unternehmen und die gesellschaftliche Ordnung zugleich treffen können. Entscheidend ist nicht allein, ob diese Angriffe verhindert werden können. Entscheidend ist auch, wie schnell und wirksam Staat, Wirtschaft und Gesellschaft im Ernstfall reagieren.

Resilienz beschreibt grundsätzlich die Fähigkeit, Krisen standzuhalten, ihre Auswirkungen zu begrenzen, sich an neue Bedingungen anzupassen und zentrale Funktionen schnell wiederherzustellen. Digitale Resilienz geht über klassische IT-Sicherheit hinaus. Sie umfasst die Fähigkeit, kritische Infrastrukturen, Verwaltungen, Kommunikation und Versorgungssysteme, gesellschaftliche Strukturen und wirtschaftliche Prozesse auch unter massiver Belastung aufrechtzuerhalten. Sie entscheidet darüber, ob unsere Infrastrukturen, Staat, Wirtschaft und Gesellschaft auch in überraschenden Krisensituationen handlungs- und funktionsfähig bleiben.

83%

der Unternehmen und 82 Prozent der Bevölkerung halten eine ernsthafte Krise infolge hybrider Angriffe für wahrscheinlich.

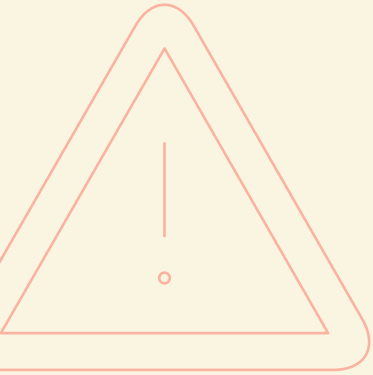
↗ Studienbericht: Hybride Angriffe (2026)



Resilienz entsteht nicht durch Abschottung, sondern durch Prävention, Modernisierung und technologische Handlungsfähigkeit. Dazu gehören sichere und leistungsfähige Infrastrukturen, gut ausgebildete digitale Kompetenzen in der Gesellschaft, durchgängig digital arbeitende Verwaltungen und technologische Souveränität der Unternehmen.

Digitale Resilienz muss als Querschnittsaufgabe verankert werden. Sie ist nicht nur Sicherheits-, sondern Modernisierungs- und Innovationspolitik, Medien- und Bildungspolitik. Staaten und Volkswirtschaften bleiben nur dann handlungsfähig, wenn sie digitale Technologien schnell adaptieren, skalieren und sicher betreiben können. Investitionen in Digitalisierung, Künstliche Intelligenz, Cloud, Cybersicherheit und digitale Kompetenzen sind Investitionen in die Resilienz eines Gemeinwesens.

Die Nationale Sicherheitsstrategie aus dem Jahr 2023 spiegelt bereits ein umfassenderes Sicherheitsverständnis wider. Der schwarz-rote Koalitionsvertrag knüpft daran an und betont die Bedeutung von Resilienz, digitaler Souveränität und dem Schutz kritischer Infrastrukturen als Bestandteil zeitgemäßer Sicherheitspolitik. Mit dem »Pakt für den Bevölkerungsschutz« sind erste Schritte zur besseren Ausstattung und Vernetzung im Katastrophen- und Zivilschutz getan.



Zudem soll der Nationale Sicherheitsrat Deutschlands strategische Handlungsfähigkeit verbessern. Damit diese Architektur wirksam wird, muss die Stärkung unserer Resilienz im Digitalen künftig systematischer mitgedacht und als ressortübergreifende Aufgabe verstanden werden.

Digitale Resilienz kann mittel- und langfristig nur im Verbund mit europäischen Partnern erreicht werden. Deutschland sollte seine Aktivitäten im Bereich Resilienz eng mit europäischen Initiativen verzahnen, gemeinsame Standards vorantreiben und digitale Souveränität als europäisches Konzept verstehen.

Dieses Bitkom-Positionspapier zeigt auf, was jetzt zu tun ist, damit Deutschland im Ernstfall handlungsfähig bleibt und wie Digitalisierung dazu beitragen kann – über Infrastrukturen, Gesellschaft, Wirtschaft und Staat hinweg.

1 Infrastruktur

Resiliente digitale Infrastrukturen sind die Grundlage für die Handlungsfähigkeit von Wirtschaft, Staat und Gesellschaft auch im Krisenfall. Auch wenn an vielen Stellen bereits umfangreiche Sicherheits-, Notfall- und Resilienzvorkehrungen getroffen wurden, sind wir auf die zunehmenden hybriden Bedrohungen und die wachsenden wechselseitigen Abhängigkeiten kritischer Infrastrukturen noch nicht ausreichend vorbereitet. Cyberangriffe, Sabotage, Extremwetterereignisse und geopolitische Spannungen erhöhen den Handlungsdruck. Ziel müssen digitale Infrastrukturen sein, die auch unter außergewöhnlichen Belastungen funktionsfähig bleiben, mit denen Störungen schnell bewältigt und kritische Interdependenzen reduziert werden können.

85%

der Unternehmen geben an, dass ein Ausfall der Telekommunikation und Informationstechnik große Auswirkungen auf ihr Unternehmen hätte.

↗ Dataverse (2026)

Telekommunikationsnetze auch im Blackout funktionsfähig halten

Telekommunikationsnetze haben sich in vergangenen Krisen als belastbar und anpassungsfähig erwiesen. Gleichzeitig zeigt die verschärfte Bedrohungslage, dass ihre Resilienz weiter gestärkt werden muss. Die zentrale Voraussetzung dafür ist eine verlässliche Energieversorgung: Ohne Strom können Kommunikationsnetze ihre Funktion für Wirtschaft, Staat und Gesellschaft nicht erfüllen. Deshalb müssen Telekommunikationsnetze als Teil der kritischen Infrastruktur in Krisen- und Katastrophenfällen bei der Energieversorgung prioritär berücksichtigt werden. Zugleich gilt: Bevor neue Schutzpflichten geschaffen werden, sollte systematisch geprüft werden, welche Notfall-, Sicherheits- und Resilienzmaßnahmen in der Branche bereits bestehen und wie wirksam sie sind. Die Telekommunikationsunternehmen investieren schon heute umfassend in Sicherheitsorganisationen, Krisenprozesse, Notstrom- und Ersatzlösungen sowie in die laufende Weiterentwicklung ihrer Schutzkonzepte. Zusätzliche Vorgaben müssen daher verhältnismäßig, praktisch umsetzbar und mit angemessenen Übergangsfristen ausgestaltet sein. Neue Resilienz- und Sicherheitsanforderungen sollten innovationsfreundlich ausgestaltet werden und bestehende Investitions- und Ausbauziele nicht gefährden. Doppelregulierung, widersprüchliche Vorgaben und unnötige Bürokratielasten müssen vermieden werden, damit Unternehmen weiterhin in Netzausbau, Modernisierung und Sicherheitsinnovationen investieren können. Sofern mit neuen Vorgaben erhebliche zusätzliche Kosten verbunden sind, braucht es zudem eine faire Verteilung der Lasten zwischen Staat, Betreibern und weiteren betroffenen Akteuren, damit Investitionsfähigkeit und Netzausbau nicht beeinträchtigt werden. Ein moderner breitbandfähiger Digitalfunk bildet zudem die Einsatzrealität von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) adäquat ab. Die Kommunikation von BOS im Krisenfall muss »omni-resilient« sein, also eine Kombination aus eigenem Kernnetz und kommerziellen Mobilfunknetzen bieten.

Digitale Infrastruktur gegen physische Angriffe wappnen

Digitale Infrastruktur ist immer auch physische Infrastruktur. Rechenzentren, Mobilfunkstandorte, Glasfaser- und Telekommunikationsleitungen sowie zentrale Netzknoten müssen deshalb wirksam gegen Sabotage, Drohnen und andere physische Bedrohungen geschützt werden. Die jüngsten Angriffe auf Rechenzentren im Nahen Osten zeigen, dass auch hochverfügbare Infrastrukturen gezielt getroffen werden können und ausreichende Redundanzen entscheidend sind. Betreiber kritischer digitaler Infrastrukturen müssen Gefahren frühzeitig erkennen und ihre Anlagen wirksam schützen können. Dazu braucht es insbesondere rechtssichere Möglichkeiten zur Drohnendetektion und gegebenenfalls auch zur Drohnenabwehr. Zudem müssen Sicherheitsbehörden relevante Lageinformationen frühzeitig mit den Betreibern teilen, Zuständigkeiten im Ernstfall klar geregelt und schnelle staatliche Unterstützung gewährleistet sein. Neben externen Angriffen müssen auch Bedrohungen im Inland, etwa durch gezielte Sabotage oder vorsätzliche Beschädigungen, stärker in den Blick genommen werden. Zudem braucht es ein gemeinsames, aktuelles und belastbares Lagebild von Staat und Betreibern, in dem konkrete Gefährdungen, Vorfälle und Angriffsmuster zusammengeführt und bewertet werden. Sicherheitsrelevante Erkenntnisse müssen so frühzeitig und konkret geteilt werden, dass Betreiber gefährdete Anlagen und mögliche Angriffswege erkennen und ihre Schutzmaßnahmen entsprechend anpassen können. Zuständigkeiten im Ernstfall müssen klar geregelt und schnelle staatliche Unterstützung gewährleistet sein.

Rechenzentren massiv ausbauen und resilienter machen

4× mehr Rechenzentrumskapazität

Die USA bauen pro Jahr viermal mehr Rechenzentrumskapazitäten neu auf, als in Deutschland insgesamt vorhanden sind.

↗ Studie Rechenzentren (2024)

Rechenzentren sind das Rückgrat der digitalen Infrastruktur und damit zentral für Daseinsvorsorge, wirtschaftliche Wertschöpfung sowie staatliche Handlungsfähigkeit. In einer digitalisierten Welt ist Resilienz untrennbar mit der digitalen Infrastruktur verbunden, denn digitale Daten und Dienste sind am Ende immer physisch. Ohne starken Ausbau der physischen Grundlage riskiert Deutschland, dass sich bestehende Abhängigkeiten weiter verschärfen und den Einfluss auf wesentliche Bereiche von Staat, Wirtschaft und Gesellschaft zu verlieren. Daher braucht es Rahmenbedingungen, die den Ausbau fördern, insbesondere schnellere Planungs- und Genehmigungsverfahren, eine sichere und bezahlbare Energieversorgung sowie investitionsfreundliche und praxistaugliche regulatorische Vorgaben. Effizienz-, Nachhaltigkeits- und Flexibilitätsanforderungen müssen so ausgestaltet werden, dass hochverfügbare und georedundante Betriebsmodelle möglich bleiben. Für Krisen braucht es klar definierte Prozesse, damit Zuständigkeiten, Priorisierungen und Eskalationswege für kritische digitale Infrastrukturen im Ernstfall eindeutig geregelt sind.

Stromnetze digital steuern

Ein resilientes Energiesystem ist Grundvoraussetzung für die Resilienz nahezu aller anderen KRITIS-Bereiche – von Kommunikationsnetzen über Gesundheitsversorgung bis zur Wasserversorgung. Angesichts zunehmender Bedrohungen durch Cyberangriffe, steigende Komplexität und geopolitische Spannungen rückt seine Stabilität stärker in den Fokus.

Digitale Technologien spielen dabei eine Schlüsselrolle: Stromnetze und dezentrale Anlagen lassen sich ohne digitale Überwachung und robuste Cybersicherheitsmaßnahmen weder zuverlässig absichern noch stabil betreiben. Die zunehmende Verzahnung von IT- und Betriebstechnologie ermöglicht zugleich die frühzeitige Erkennung von Störungen, schnellere Fehlerlokalisierung und automatisierte Wiederherstellung im Krisenfall.

Digitale Technologien sollten deshalb als integraler Bestandteil resilienter Energieinfrastrukturen verstanden und entsprechend gefördert werden. Netzbetreiber benötigen bessere Rahmenbedingungen für Investitionen in digitale Lösungen und Zugang zu hochwertigen Echtzeitdaten. Gleichzeitig sollten geopolitische Abhängigkeiten durch erneuerbare Energien, eine diversifizierte Technologiebasis und den erleichterten Einsatz von KI zur Netzstabilisierung reduziert werden.

Digitale Verkehrssteuerung ausbauen

Digitalisierte Verkehrsinfrastrukturen sind ein entscheidender Faktor unserer Resilienz. In Krisensituationen können Staus, fehlende Echtzeitdaten oder unzureichend vernetzte Verkehrssysteme die Mobilität von Rettungskräften sowie die Logistik erheblich beeinträchtigen. Gleichzeitig verzögern analoge Planungs- und Genehmigungsverfahren häufig die schnelle Wiederherstellung beschädigter Verkehrsinfrastruktur. Planungs- und Genehmigungsprozesse im Straßen- und Schienenverkehr sollten daher vollständig digitalisiert werden, das Infrastruktur-Zukunftsgesetz ist hierzu ein wichtiger erster Schritt. Darüber hinaus braucht es eine bundesweit abgestimmte Strategie zur Digitalisierung der Verkehrsinfrastruktur und Bereitstellung der Daten mit klar definierten Etappen und KPIs – das schließt insbesondere digitale Verkehrssteuerungssysteme ein, die Störungen frühzeitig erkennen und eine dynamische Priorisierung kritischer Verkehre ermöglichen.

Interoperabilität im Gesundheitswesen stärken

Die Digitalisierung des Gesundheitswesens hat Fortschritte gemacht, die Krisenfähigkeit der Systeme jedoch nicht im gleichen Maße. Krankenhausinformationssysteme, Rettungsleitstellen und Behörden arbeiten vielerorts weiterhin mit inkompatiblen Datenformaten und Schnittstellen – mit Risiken für Versorgung und Koordination im Ernstfall.

Interoperabilitätspflichten im Gesundheitswesen müssen deshalb konsequent auch unter Resilienzkriterien definiert werden. Die elektronische Patientenakte, digitale Kommunikationslösungen und Telematikinfrastruktur sollten so verzahnt werden, dass Notfallzugriffe und Datenschutz gleichzeitig in Echtzeit gewährleistet sind.

Die geplante Reform der Notfallversorgung setzt hierfür wichtige Impulse durch stärkere digitale Vernetzung, telemedizinische Angebote und die Anbindung von Rettungsdiensten an die Telematikinfrastruktur.

Interoperabilität sollte dabei auf Basis internationaler Standards gesichert werden, um auch grenzüberschreitende Krisen- und Notfallszenarien zuverlässig bewältigen zu können. Außerdem braucht es klare Governance-Strukturen für die digitale Gesundheitsversorgung: Eine dauerhafte, ressort- und sektorenübergreifende Koordination kann sicherstellen, dass Standards weiterentwickelt, Innovationen schneller implementiert und alle Akteure – vom Gesundheitswesen über den Katastrophenschutz bis hin zur Verteidigung – enger verzahnt zusammenarbeiten.

2 Gesellschaft

Hybride Angriffe sind auch deswegen so gefährlich für Deutschland, weil sie die Stabilität unserer Gesellschaft und das Vertrauen in den Staat gezielt unterminieren sollen. Wir sind Ziel fortgesetzter Desinformationskampagnen: Rund 90 Prozent der Deutschen begegnen im Alltag Fake News, ein Drittel davon zu Politik in Deutschland.[1] Die Verbesserung von digitaler Resilienz und demokratischer Widerstandsfähigkeit aller Bürgerinnen und Bürger muss daher prioritäres Ziel staatlicher Krisenvorsorge und -abwehr sein. Die deutsche Gesellschaft muss in der Breite sehr viel stärker für die Mechanismen hybrider Angriffe und Deutschlands konkrete Bedrohungslage sensibilisiert werden. Nur eine digital resiliente Gesellschaft wird nicht selbst zum Spielball derjenigen, die das Gemeinwesen zu schwächen versuchen.

63%

der Befragten vertrauen darauf, dass die Bevölkerung im Fall von hybriden Angriffen umfassend informiert wird.

↗ Studienbericht (2026)

Krisenkommunikation und Warnsysteme modernisieren

Im Ernstfall entscheiden Minuten. Wer die Bevölkerung nicht rechtzeitig und zuverlässig warnen kann, verliert wertvolle Zeit. Digitale Technologien und Kommunikation sind im Krisenfall entscheidend. Trotz spürbarer Verbesserungen seit dem Warntag 2020 bestehen im deutschen Warnsystem weiterhin strukturelle Schwächen. Cell Broadcast ist ein wichtiger Schritt, reicht allein jedoch nicht aus. Deutschland sollte den bestehenden Warnmix zu einem Multichannel-Warnsystem weiterentwickeln und neben Cell Broadcast, NINA und Rundfunk auch auf digitale Displays in Bahnhöfen, an Haltestellen oder auf Werbeflächen zurückgreifen. Zentrale Warnungen müssen medienbruchfrei aus einem gemeinsamen System gespeist werden, um alle Bürgerinnen und Bürger zu erreichen. Warnungen sollten präzise und handlungsorientiert formuliert sowie barrierefrei und mehrsprachig ausgespielt werden. Staatliche Kommunikationskanäle müssen dennoch auch beim Ausfall digitaler Infrastrukturen funktionieren. Dafür braucht es eine deutliche Erhöhung der Testfrequenz, orientiert an internationalen Vorbildern wie den Niederlanden, wo öffentliche Warnsirenen monatlich überprüft werden. Zusätzlich braucht es eine Kommunikationskampagne, die alle Bürgerinnen und Bürger mit den gängigen Warnkanälen bekannt und vertraut macht.

Die Bevölkerung muss außerdem kognitiv auf schwere Krisen und einen möglichen Kriegsfall vorbereitet sein, wie es Schweden und Finnland seit Jahren vorbildhaft praktizieren. Krisenkompetenz sollte auch in Deutschland systematisch im Alltag verankert werden: durch verbindliche Vorsorge in Schulen, regelmäßige Krisenübungen in Kommunen, Verwaltungen und kritischen Infrastrukturen, leicht verständliche Handlungsempfehlungen für Haushalte sowie wiederkehrende Informationskampagnen über öffentlich-rechtliche Rundfunkanstalten, digitale Warnkanäle und lokale Vertrauensakteure.

1 ↗ Bitkom Research, 2026.

Denkbar wäre in Deutschland die Koordination dieser Aktivitäten durch eine eigene Agentur zur Stärkung der psychologischen Resilienz der Bevölkerung nach schwedischem Vorbild (Swedish Psychological Defense Agency). Eine solche Agentur könnte unter anderem kurzfristig eine Infokampagne zur aktuellen hybriden Bedrohungslage unter Beteiligung der Wirtschaft umsetzen, um die Bevölkerung zu sensibilisieren.

Die Prognosefähigkeit staatlicher Stellen muss durch den Einsatz KI-gestützter Frühwarnsysteme zudem deutlich verbessert werden. Kommunale und regionale Versorger sind als Kommunikatoren und lokale Vertrauensanker systematisch in die Krisenkommunikation einzubeziehen. Die Politik sollte das modulare Warnsystem gezielt modernisieren und lokale Anpassungen von Textbausteinen ermöglichen, um situationsgerechte und präzise Kommunikation sicherzustellen.

Verbreitung von Desinformation bekämpfen

63%

der Befragten gaben an, Desinformation insbesondere zu Themen, wie Migration, dem Ukraine-Krieg und dem Israel-Gaza-Konflikt wahrgenommen zu haben.

↗ Social Media und Desinformation (2026)

Desinformationskampagnen sind kein neues Phänomen, aber ihre Wirksamkeit hat sich durch KI-generierte Inhalte grundlegend verändert. Koordinierte Manipulationsoperationen untergraben das Vertrauen in staatliche Institutionen, demokratische Prozesse und digitale Dienste. Ihre Bekämpfung von Desinformation ist eine gesamtgesellschaftliche Aufgabe. Politik, Zivilgesellschaft und Wirtschaft müssen gemeinsam dazu beitragen, Medienkompetenz zu stärken, Faktenchecks und Aufklärung auszubauen sowie technische Lösungen zur Erkennung manipulierter Inhalte weiterzuentwickeln.

Gerade die Digitalwirtschaft leistet mit Innovationen zur Deepfake-Erkennung und automatisierter Analyse KI-generierter Inhalte einen wichtigen Beitrag zur digitalen Resilienz. Die Forschung zu KI-generierten Inhalten und automatisierten Erkennungsverfahren ist deshalb gezielt zu fördern. Desinformationskampagnen sollten außerdem in ein übergreifendes, smartes Lagebild zu hybriden Bedrohungen einfließen, ebenso wie Cybersicherheit und Drohnensichtungen.

Um organisierte Desinformationskampagnen, die die staatliche und demokratische Handlungsfähigkeit ins Visier nehmen, frühzeitig adressieren zu können, sollte sogenanntes »Prebunking« zum festen Bestandteil staatlicher Krisenkommunikation werden. Insbesondere bei absehbaren Krisen und Manipulationsmustern sollten von offiziellen Stellen frühzeitig Fakten, typische Falschmeldungsmethoden und verlässliche Informationsquellen erklärt werden, bevor Desinformation eine größere Reichweite erzielen kann. Die Bundesregierung könnte sich hier am Positivbeispiel Taiwan und dem dort gelebten 60-Minuten-Konzept zur Verbreitung von Aufklärungsnarrativen orientieren.

Einen wichtigen Beitrag zur Bekämpfung von Desinformation und systemischen Risiken leistet zudem eine konsequente Anwendung und Durchsetzung des bestehenden europäischen Rechtsrahmens. Dazu gehört insbesondere die Durchsetzung des Digital Services Act (DSA) weiter zu stärken, indem die zuständigen nationalen Aufsichtsstrukturen mit den notwendigen Ressourcen ausgestattet werden.

Aktuell ist der deutsche Digital Services Coordinator (DSC) unterbesetzt und damit in seinen Fähigkeiten eingeschränkt. Zugleich sollte das Trusted-Flagger-System weiter ausgebaut und gestärkt werden, damit rechtswidrige Inhalte schnell und verlässlich identifiziert und gemeldet werden können. Ergänzend gilt es, den »Code of Conduct on Disinformation« als wichtiges Instrument der Ko- und Selbstregulierung weiterzuentwickeln und seine praktische Wirksamkeit zu stärken. Entscheidend ist ein kohärenter europäischer Ansatz, der bestehende Instrumente wirksam nutzt, statt zusätzliche parallele Regelungsstrukturen zu schaffen.

Erkennung von Desinformation verbessern

Gesellschaftliche Resilienz setzt insbesondere vor dem Hintergrund der gezielten Angriffe auf gesellschaftliche Stabilität voraus, dass Menschen digitale Dienste sicher nutzen, Informationen einordnen, Desinformation erkennen und im Krisenfall richtig reagieren können. Allerdings sind Medien- und Digitalkompetenzen in Deutschland je nach Alter, Region und Bildungshintergrund ungleich verteilt und ein systematischer Ansatz, sie zu stärken, fehlt bisher. Deutschland braucht daher eine »Nationale Strategie zur Stärkung von Medien- und Digitalkompetenzen«, die Bildungseinrichtungen, Zivilgesellschaft, Plattformen und Medien zusammenbringt sowie alle Altersgruppen adressiert. Medien- und Digitalkompetenzen müssen in der gesamten Bundesrepublik in allen Klassenstufen systematisch unterrichtet werden.

Hinzu kommt der Aus- und Weiterbildungsbedarf von Lehrkräften. Der Bereich Medienkompetenz, digitale Resilienz und Umgang mit Desinformation muss verpflichtender Bestandteil von Lehramtsstudium, Vorbereitungsdienst und Lehrkräftefortbildung werden. Bund und Länder sollten gemeinsam digitale Fortbildungsangebote, Materialien und Qualitätsstandards entwickeln, die von allen Lehrkräften in Deutschland genutzt und umgesetzt werden. Koordinieren könnte diese Gesamtstrategie eine Bundeszentrale für digitale Bildung. Als Positivbeispiel kann Finnland mit seiner altersübergreifenden Medienkompetenzstrategie fungieren.

Für die breite Bevölkerung müssen in Kooperation mit der Wirtschaft und zivilen Einrichtungen wie Wohlfahrtsverbänden, Sportvereinen, Volkshochschulen oder Bibliotheken entsprechende Angebote geschaffen beziehungsweise ausgebaut werden. Notwendig sind niedrigschwellige Informations- und Bildungsangebote in der Fläche. Ein erster Schritt hierzu wäre die Aufnahme von Digital- und Medienkompetenz in die Weiterbildungsgrundversorgung der Volkshochschulen, wie Nordrhein-Westfalen es bereits in seinem Landesweiterbildungsgesetz vorgesehen hat. Andere Länder sollten diesem Beispiel folgen. Um zudem ehrenamtliches Engagement im Sinne einer resilienten, digitalen Gesellschaft zu stärken und systematisch mit dem Erwerb digitaler und Medienkompetenzen zu verknüpfen, braucht es eine neue Säule im Bundesfreiwilligendienst: den Bundesdigitaldienst, offen ab 16 Jahren, für eine Dauer von 6 bis 24 Monaten mit Bildungs- und Ehrenamtsmodulen.

Digitale Resilienz erfordert außerdem ausreichend Fachkräfte in Cybersicherheit, KI, Softwareentwicklung und digitaler Infrastruktur. Bund und Länder sollten daher gemeinsam mit der Wirtschaft eine Fachkräfteoffensive für digitale Schlüsselkompetenzen entwickeln – von Schule, Ausbildung und Studium bis zur berufsbegleitenden Weiterbildung und gezielten internationalen Fachkräftegewinnung. Bestandteil könnte unter anderem die Entwicklung eines neuen Ausbildungsberufs »Fachinformatiker/Fachinformatikerin für Cybersicherheit« sein, der bislang nicht existiert.

3 Wirtschaft

Deutschland verfügt in Teilen der Wirtschaft bereits über viel Sicherheits-Know-How. Viele Unternehmen setzen sich bereits intensiv mit der veränderten Sicherheitslage auseinander und stärken ihre Vorsorge. So wollen 37 Prozent der Unternehmen künftig stärker in die Vorbereitung auf hybride Angriffe investieren. Gleichzeitig verfügen viele Unternehmen mit etablierten Standards für Business Continuity Management bereits über Strukturen, um auf Krisen und Störungen vorbereitet zu sein und ihre Widerstandsfähigkeit kontinuierlich zu stärken. Damit bestehen in der Wirtschaft bereits wichtige Grundlagen für mehr Resilienz. Entscheidend ist nun, diese Ansätze in die Breite zu tragen, insbesondere auch zu Unternehmen, die kritische Versorgungsinfrastrukturen betreiben, und sie zugleich an das veränderte Bedrohungsbild anzupassen. Denn Unternehmen müssen heute nicht nur gegen klassische Betriebsunterbrechungen, sondern ebenso gegen Desinformation, Cyberattacken, physische Angriffe und Wirtschaftsspionage gewappnet sein. Der Zugang zu neuesten Sicherheitstechnologien, eine konkurrenzfähige nationale Sicherheitswirtschaft und sichere Lieferketten sind weitere wichtige Bausteine für die Resilienz der Wirtschaft.

96%

der Unternehmen sind von Datendiebstahl, Industriespionage oder Sabotage betroffen oder vermuten entsprechende Vorfälle.

↗ Wirtschaftsschutz | Studie 2026

Cyberrisiken systematisch begegnen

Cyberangriffe verursachen in Deutschland bereits heute jährlich Schäden in dreistelliger Milliardenhöhe. Kleine und mittlere Unternehmen sind dabei besonders betroffen, weil sie seltener über eigene Sicherheitsressourcen verfügen und gezielt als Einstiegspunkt in größere Lieferketten genutzt werden. Koordinierte Angriffsszenarien, bei denen Rechenzentren, Internetknoten, Umspannwerke oder Stellwerke ausfallen, verdeutlichen die Verwundbarkeit einer hochvernetzten Volkswirtschaft.

Cybersicherheit ist deshalb nicht länger eine Spezialfrage der IT, sondern die operative Grundlage staatlicher, wirtschaftlicher und gesellschaftlicher Resilienz. Die Bundesregierung sollte ein einheitliches Cyberlagebild bereitstellen, das Behörden und Unternehmen in einen echten bidirektionalen Informationsfluss bringt und Lageerkenntnisse nicht nur staatlich sammelt, sondern wirtschaftsnah nutzbar macht. Dafür sollten insbesondere die Meldedaten aus dem BSI-Portal systematisch einbezogen und mit den Erkenntnissen des Abwehrzentrums gegen hybride Bedrohungen verknüpft werden.

Disruptive Entwicklungen in kritischen Technologien erfordern konkrete Antworten, insbesondere im Bereich der Künstlichen Intelligenz und des Quantencomputings. KI kann die Cybersicherheit stärken, indem sie Angriffe schneller erkennbar macht, Prozesse automatisiert und die Reaktionsfähigkeit verbessert. Zugleich verschärft sie die Bedrohungslage. Deshalb sind die Einrichtung des nationalen KI-Sicherheitsinstituts AISI Deutschland sowie die Sicherstellung des Zugangs zu den neuesten Frontier-Modellen wichtige Schritte.

Entscheidend ist jetzt, dass AISI Deutschland mit den nötigen Kompetenzen und finanziellen wie personellen Ressourcen ausgestattet und als Technologie-Startup innerhalb der Regierung ausgestaltet wird. Außerdem sind gezielte Investitionen in resiliente KI-Infrastrukturen, vertrauenswürdige Modelle und sichere Anwendungen für kritische Infrastrukturen notwendig. Fortschritte bei der Entwicklung von Quantencomputern erfordern Antworten, insbesondere mit Blick auf künftige Risiken für Verschlüsselung, Kommunikation und digitale Souveränität.

Anreize und Förderungen für Cybersicherheitsinvestitionen erhöhen

Zu oft scheuen Unternehmen und insbesondere KMU hohe Investitionen in Cybersicherheit, nur um im Schadensfall mit deutlich höheren Kosten konfrontiert zu werden. Deshalb braucht es stärkere finanzielle Anreize für den Einsatz von Cybersicherheitslösungen. Dazu gehören insbesondere steuerliche Abschreibungen für neu beschaffte Produkte, Dienstleistungen und Schulungen sowie direkte Förderprogramme zur Stärkung der Cybersicherheit. Insbesondere KMU in kritischen Sektoren sollten von solchen Maßnahmen profitieren, indem sie möglichst bürokratie- und aufwandsarm ausgestaltet werden.

Auch Startups im Bereich Cybersicherheit sollten gezielt durch Steuererleichterungen, Mietzuschüsse und besseren Zugang zu Technologien unterstützt werden. Darüber hinaus muss das Forschungsrahmenprogramm »Digital. Sicher. Souverän.« über 2026 hinaus verlässlich fortgeführt werden. Ein Auslaufen oder längere Unterbrechungen würden Deutschlands und Europas Fähigkeit schwächen, sicherheitskritische Schlüsseltechnologien eigenständig zu entwickeln. Gerade angesichts der schnellen Fortschritte bei KI und der strategischen Bedeutung von Quantensicherheit braucht es langfristige Planungssicherheit für Forschung, Transfer und Nachwuchsgewinnung. Unsichere Förderperspektiven gefährden bestehende Kompetenzen, treiben Talente in besser finanzierte Märkte oder ins Ausland und schwächen die technologische Souveränität Europas.

Geheimschutz digitalisieren und Verfahren vereinheitlichen

Ein praxistauglicher Geheimschutz ist Voraussetzung dafür, dass Unternehmen sicherheits- und verteidigungsrelevante Technologien schnell bereitstellen können. Hohe Sicherheitsstandards und schnelle Lieferfähigkeit dürfen dabei kein Gegensatz sein. Unternehmen müssen sich frühzeitig auf Geheimschutzanforderungen vorbereiten können. Dafür sollten das Geheimschutzhandbuch modernisiert, Anforderungen verständlich und digital zugänglich gemacht sowie die Aufnahme in die Geheimschutzbetreuung und Sicherheitsüberprüfungen durchgängig digitalisiert werden.

Gleichzeitig braucht es einheitliche Verfahren über Behörden und föderale Ebenen hinweg. Gültige Sicherheitsüberprüfungen sollten grundsätzlich personenbezogen sowie behörden-, bund- und länderübergreifend anerkannt und Unternehmen mit mehreren Bedarfsträgern durch eine federführende Stelle zentral betreut werden. Ausreichende personelle Ressourcen und einheitliche Bewertungsmaßstäbe müssen die Verfahren zusätzlich beschleunigen. So wird Geheimschutz zum Enabler für Innovation und schnelle Lieferfähigkeit, ohne das Sicherheitsniveau abzusenken.

Halbleiter-Lieferketten wettbewerbsfähig aufstellen

60%

der Unternehmen, die 2025 Halbleiter gekauft haben, berichten von Schwierigkeiten bei der Beschaffung.

↗ Studienbericht (2025)

Halbleiterkomponenten sind eine unverzichtbare Grundlage für digitale Infrastrukturen, industrielle Produktion, Medizintechnik und Verteidigungsfähigkeit. Störungen in Halbleiter-Lieferketten können daher nicht nur einzelne Unternehmen treffen, sondern auch Produktion und die Funktionsfähigkeit zentraler Systeme beeinträchtigen. Wir wissen, wie anfällig Wirtschaft und Industrie gegenüber geopolitischen Spannungen in komplexen globalen Halbleiter-Lieferketten sind. Resilienz in der Mikroelektronik bedeutet deshalb nicht Abschottung, sondern den gezielten Aufbau wettbewerbsfähiger Strukturen entlang der gesamten Wertschöpfungskette in Deutschland und Europa – von Design und Entwicklung über Fertigung bis hin zu Materialien, Chemikalien, Ausrüstung und Fachkräften. Zugleich müssen internationale Bezugsquellen diversifiziert, strategische Abhängigkeiten reduziert und europäische Stärken so ausgebaut werden, dass belastbare internationale Interdependenzen entstehen. Dazu gehört auch, die Rahmenbedingungen für Investitionen, Innovation und Skalierung verlässlich auszugestalten, damit neue Generationen mikroelektronischer Technologien schneller in Europa zur Anwendung gebracht und kommerzialisiert werden können.

Fast Track für DefTech-Startups schaffen

Innovative Startups und Scaleups aus den Bereichen Defense, Cybersicherheit, KI, Quantencomputing und Dual-Use-Technologien sind für die technologische Souveränität Deutschlands von strategischer Bedeutung. Ihr Marktzugang wird jedoch durch lange Beschaffungsverfahren, hohe Einstiegsbarrieren und fehlende Pilotierungsmöglichkeiten erschwert. Das schwächt den Innovationsstandort und verzögert den Transfer sicherheitsrelevanter Technologien in die Praxis.

Ein Fast-Track-Verfahren sollte daher schnell umgesetzt werden: mit klaren Ansprechpartnern, offenem Zugang für Startups und Scaleups, schnellen Pilotierungen, skalierbaren SaaS-Rahmenverträgen und einem zentralen Marktplatz für DefTech- und Dual-Use-Lösungen. Gleichzeitig sollte der Beitrag zur gesellschaftlichen Resilienz als verbindliches Förderkriterium in Innovationsprogrammen verankert werden. Wagniskapital für sicherheitsrelevante Technologien muss strukturell zugänglicher werden – über bessere Beteiligungsmöglichkeiten institutioneller Investoren und gezielte öffentliche Kofinanzierung.

90%

der im ↗ Bitkom DefTech Report 2026 befragten DefTech- und Dual-Use-Gründerinnen und -Gründer bewerten die Relevanz von Fast-Track-Verfahren als hoch oder sehr hoch.

Digitalanteil an den Verteidigungsausgaben erhöhen

Der Koalitionsvertrag hat sich zum Ziel gesetzt, Zukunftstechnologien für die Bundeswehr verstärkt zu fördern. Die aktuelle Haushaltsrealität ist jedoch eine andere: Zwar wurden in den Jahren 2025 und 2026 hohe Mittel für einzelne Digital- und Zukunftsprojekte eingeplant, aber häufig mit langfristiger Mittelbindung, deren operative Wirkung erst verzögert eintritt. Ein Großteil der Verteidigungsausgaben fließt weiterhin in klassische Systeme. Das zeigt sich auch am Anteil der Ausgaben für Digitalisierung und Zukunftstechnologien: Dieser lag in den vergangenen Jahren nur bei fünf bis neun Prozent. Verteidigungsfähig wird aber nur, wer digital führend ist. Die Diskrepanz der Mittelvergabe führt dazu, dass die digitale Transformation der Bundeswehr zurückbleibt und Wachstumspotenziale durch Investitionen in Zukunftstechnologiefelder nicht genutzt werden. Von höheren Ausgaben für software-definierte Fähigkeiten würden nicht nur neue Player profitieren, sondern Innovation würde insgesamt in Deutschlands Wirtschaft gefördert werden. Ab 2027 sollten daher mindestens 10 Prozent des Verteidigungshaushaltes in Digitalisierung fließen. Mindestens ein Prozent sollte für disruptive Technologien und zur Förderung von DefTech-Startups verausgabt werden.

4 Staat

Die Widerstands- und Reaktionsfähigkeit staatlicher Strukturen wird angesichts unserer Bedrohungs- und Krisenlage immer wichtiger. Viele Prozesse und Strukturen unserer Behörden sind noch nicht konsequent auf den Krisenbetrieb ausgelegt, zu fragmentiert und zu wenig interoperabel. Der Staat muss aber auch unter außergewöhnlicher Belastung entscheidungsfähig bleiben, zentrale Leistungen verlässlich erbringen, schnell auf neue Bedrohungen reagieren und mit Wirtschaft und Gesellschaft koordiniert handeln können. Dafür muss Resilienz stärker als grundlegendes Prinzip staatlicher Handlungsfähigkeit verstanden werden – von der öffentlichen IT über Sicherheitsbehörden und Beschaffung bis hin zu Gesundheits- und Rettungsstrukturen.

Resilienz-by-Design in der öffentlichen IT verankern

Die Handlungsfähigkeit des Staates im Krisenfall hängt maßgeblich von resilienten digitalen Verwaltungsprozessen ab. Bund, Länder und Kommunen sollten deshalb einen verbindlichen Katalog kritischer Verwaltungsleistungen definieren – etwa für Krisenkommunikation, Meldewesen, Gesundheits- und Katastrophenschutz, innere Sicherheit sowie staatliche Leistungen und Zahlungen. Für diese Kernprozesse müssen klare Notbetriebsverfahren, definierte Mindestservicelevels und eindeutige Entscheidungswege festgelegt werden, um staatliche Handlungsfähigkeit auch unter Belastung sicherzustellen.

Resilienz sollte dabei von Beginn an Bestandteil der IT-Architektur der öffentlichen Verwaltung sein. Dazu gehören redundante Betriebsmodelle, standardisierte Schnittstellen, regelmäßige Backup- und Wiederanlauftests sowie klare Anforderungen an Datenportabilität und Wechselmöglichkeiten bei zentralen Plattformen. Diese Vorgaben sollten deutschlandweit einheitlich und verbindlich über die IT-Architekturrichtlinien des Deutschland-Stacks durchgesetzt werden. Gleichzeitig braucht es einheitliche Krisenstrukturen und ein gemeinsames digitales Lagebild über alle föderalen Ebenen hinweg. Standardisierte Rollen, Eskalationswege und abgestimmte Kommunikationsverfahren können dazu beitragen, Entscheidungen schneller und koordinierter zu treffen, die Bürgerkommunikation zu verbessern und die staatliche Reaktionsfähigkeit nachhaltig zu stärken.

70%

der Bevölkerung sind der Meinung, dass die deutschen Behörden gar nicht gut oder eher nicht gut auf Cyberangriffe vorbereitet sind.

↗ Dataverse (2026)

EUDI-Wallet als Notfallpass nutzen

61%

der Befragten wünschen sich, Ausweis, Führerschein oder vergleichbare Karten digital auf dem Smartphone mitzuführen.

↗ Dataverse (2026)

Mit dem geplanten Start am 2. Januar 2027 bietet die EUDI-Wallet eine wichtige Chance zur Stärkung digitaler Resilienz. Sie steigert nicht nur die Sicherheit von Authentifizierungsverfahren, sondern kann auch dafür sorgen, dass wichtige Dokumente digital verfügbar sind. Dadurch sind Bürgerinnen und Bürger im Krisen- oder Katastrophenfall handlungsfähiger, gerade wenn physische Dokumente vernichtet, beschädigt oder unzugänglich sind. Durch die sichere Online- und Offline-Identifikation bleibt ihre Nutzung auch möglich, wenn Netze gestört oder nur eingeschränkt verfügbar sind. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sollte deshalb gemeinsam mit den zuständigen Ressorts ein empfohlenes Portfolio zentraler Krisendokumente definieren und dessen sichere Ablage in einem BBK-Notfall-Wallet als Use-Case für die EUDI-Wallet aktiv kommunizieren.

Die Einführung der EUDI-Wallet sollte genutzt werden, um Resilienzanforderungen von Beginn an in die Anwendungspraxis zu übersetzen. Zugleich sollte die geplante »Bw-Wallet« der Bundeswehr schnell umgesetzt und konsequent auf der Technologie der EUDI-Wallet aufbauen. Analoge Nachweise sollten schrittweise durch digitale Dokumente in der »Bw-Wallet« ersetzt und nach dem Prinzip »Digital-Only« und »Once-Only« anerkannt werden.

Fähigkeiten der Sicherheitsbehörden gezielt stärken und vernetzen

Hybride Angriffe und Cyberoperationen erfordern leistungsfähige Sicherheitsbehörden, die schnell und koordiniert handeln können. Neue Befugnisse müssen deshalb mit ausreichenden Ressourcen, eindeutigen Zuständigkeiten und einer kohärenten Verantwortungsarchitektur einhergehen. Federführung, technische Koordinierung und das Zusammenspiel der beteiligten Behörden und Ressorts sollten verbindlich geregelt werden, damit vorhandene Fähigkeiten im Ernstfall wirksam zusammenwirken.

Gleichzeitig muss die Zusammenarbeit mit der Wirtschaft zu einem festen Bestandteil staatlicher Sicherheitsvorsorge werden. Dafür braucht es einen sicheren, bidirektionalen Informationsaustausch, der Erkenntnisse zu Bedrohungen zusammenführt und konkrete, zeitnah nutzbare Informationen für Schutzmaßnahmen zurückspielt. Operative Unterstützungsfähigkeiten wie die Mobile Incident Response Teams des BSI und der gezielte Austausch handlungsrelevanter Erkenntnisse mit betroffenen Unternehmen sollten weiter gestärkt werden. Staatliche Eingriffe in technische Systeme müssen dabei klar abgegrenzt bleiben und Kooperation grundsätzlich Vorrang haben.

Beschaffung auf Krisenfälle vorbereiten

Im Krisenfall entscheidet nicht nur, was der Staat kann, sondern wie schnell er handeln kann. Fehlende Vorabvereinbarungen mit Lieferanten, unklare Vergabewege und nicht aktivierbare Kapazitätsreserven führen dazu, dass dringend benötigte IT-Leistungen und Fachkräfte im Ernstfall nicht kurzfristig mobilisiert werden können. Personal- und Beschaffungsresilienz ist bislang kein eigenständiges Planungsziel der öffentlichen Verwaltung.

Qualifizierungspfade und behördenübergreifende Expertenpools sollten aufgebaut werden, die im Krisenfall schnell aktiviert werden können. Vorkonfigurierte Beschaffungs- und Lieferkettenoptionen, Rahmenverträge und Notvergabebausteine müssen so ausgestaltet sein, dass innerhalb von 72 Stunden zusätzliche Kapazitäten und Leistungen bereitstehen. Das setzt voraus, dass diese Strukturen im Normalbetrieb gepflegt und regelmäßig getestet werden.

Sicherheitsgesetzgebung harmonisieren und praxistauglich umsetzen

Die Sicherheitsgesetzgebung der EU hat zentrale Eckpfeiler für mehr Resilienz in Europa gesetzt. NIS-2 stärkt die digitale Sicherheit von Unternehmen, das KRITIS-Dachgesetz adressiert den physischen Schutz kritischer Infrastrukturen und der Cyber Resilience Act erhöht die Cybersicherheit von Produkten mit digitalen Elementen. Entscheidend ist nun, diese Regelwerke zu einem kohärenten Sicherheitsrahmen zu verbinden. Dazu gehören unter anderem einheitliche Registrierungs- und Meldeprozesse nach NIS-2 und KRITIS-Dachgesetz. Meldungen müssen von Beginn an so verarbeitet werden, dass sie in ein gemeinsames Lagebild einfließen und einen echten bidirektionalen Informationsaustausch zwischen Staat und Wirtschaft ermöglichen. Für den CRA sind rechtzeitig verfügbare europäische harmonisierte Normen zwingend notwendig, um eine konsequente Umsetzung zu gewährleisten und Lieferengpässe zu vermeiden. Nur wenn die rechtlichen Pflichten zusammengedacht werden, entstehen aus europäischen Resilienzvorgaben praxistaugliche, rechtssichere und wirksame Schutzmechanismen.

Mehr als **211 Milliarden** Euro

Schaden durch Datendiebstahl, Industriespionage und Sabotage.

↗ Wirtschaftsschutz | Studie 2026

Rettungskette digital steuern

Das Gesundheitswesen in Deutschland ist auf komplexe und schwere Krisenszenarien nicht ausreichend vorbereitet. Nicht nur die Bundeswehr, sondern auch zivile Hilfsorganisationen, Rettungsdienste und Krankenhäuser benötigen im Krisenfall eine digitalisierte und steuerungsfähige Rettungskette.

Dafür sollte entlang der gesamten militärisch-zivilen Rettungskette ein harmonisiertes, interoperables und mit NATO-Standards kompatibles digitales Dokumentations- und Steuerungssystem eingeführt werden. Papierbasierte Prozesse könnten dadurch ersetzt, Informationsflüsse beschleunigt und Echtzeit-Lagebilder ermöglicht werden.

Ein solches Steuerungssystem würde zudem eine koordinierte Patientenlenkung erleichtern. Digitale Plattformen und Lageinformationen könnten helfen, Behandlungskapazitäten transparent darzustellen und Patientinnen und Patienten bedarfsgerecht zu verteilen – insbesondere bei Großschadenslagen oder militärisch-zivilen Einsatzszenarien.

Neue Technologien können die Leistungsfähigkeit der Rettungskette zusätzlich steigern. KI-gestützte Systeme ermöglichen schnellere Triage- und Entscheidungsprozesse, während digitale Identitätslösungen eine eindeutige Zuordnung von Patientendaten sicherstellen können.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom