TELEKOMMUNIKATION

Strategie-papier

Resilienz der
Telekommunikationsnetze

Bundesnetzagentur

Strategiepapier Resilienz der Telekommunikationsnetze

Version 1.9

Stand: November 2026

**Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen**

Abteilung 2

Tulpenfeld 4
53113 Bonn
E-Mail: notfallvorsorge@bnetza.de

Inhaltsverzeichnis

Inhaltsverzeichnis 3
1 Einleitung 5
2 Beschreibung der betrachteten Szenarien 7
2.1 Störung der Energieversorgung 7
2.1.1 Beschreibung des Szenarios 7
2.1.2 Auswirkungen des Szenarios 7
2.1.3 Bewertung des Szenarios 8
2.2 Naturkatastrophen 8
2.2.1 Beschreibung des Szenarios 8
2.2.2 Auswirkungen des Szenarios 9
2.2.3 Bewertung des Szenarios 9
2.3 Wirtschaftliche Engpasssituationen 9
2.3.1 Beschreibung des Szenarios 9
2.3.2 Auswirkungen des Szenarios 10
2.3.3 Bewertung des Szenarios 10
2.4 Hybride Bedrohungslagen 10
2.4.1 Beschreibung des Szenarios 10
2.4.2 Auswirkungen des Szenarios 10
2.4.3 Bewertung des Szenarios 11
2.5 Unruhen 11
2.5.1 Beschreibung des Szenarios 11
2.5.2 Auswirkungen des Szenarios 11
2.5.3 Bewertung des Szenarios 12
2.6 Kriegerische Auseinandersetzungen 12
2.6.1 Beschreibung des Szenarios 12
2.6.2 Auswirkungen des Szenarios 13
2.6.3 Bewertung des Szenarios 13
2.7 Fehlende Souveränität bei der Nutzung von IT- und TK-Technologie 14
2.7.1 Beschreibung des Szenarios 14
2.7.2 Auswirkungen des Szenarios 14
2.7.3 Bewertung des Szenarios 15
2.8 Menschliches Versagen 15
2.8.1 Beschreibung des Szenarios 15
2.8.2 Auswirkungen des Szenarios 16
2.8.3 Bewertung des Szenarios 16
2.9 Pandemien 16
2.9.1 Beschreibung des Szenarios 16
2.9.2 Auswirkungen des Szenarios 17
2.9.3 Bewertung des Szenarios 17
2.10 Interdependenzen der Auswirkungen aller Szenarien 17
3 Ableitung resilienzsteigernder Maßnahmen bzw. Gestaltungsoptionen 19
3.1 TK-bezogene Maßnahmen 19
3.1.1 Grundsicherung der Kommunikationsfähigkeit in Krisensituationen 19
3.1.2 Erhöhung der Verfügbarkeit im Sinne der §§ 164, 185 in Verbindung mit § 167 TKG 21

3.1.3 Einbeziehung satellitengestützter Lösungen 22
3.1.4 Erhöhung der Verfügbarkeit der Kommunikationsmöglichkeiten der Behörden 23
3.2 Notruf und öffentliche Warnungen 24
3.3 Organisatorische Gestaltungsoptionen des Krisenmanagements an der Nahtstelle zur Telekommunikation 25
3.3.1 Bevölkerungs- und Katastrophenschutz bzw.Zusammenarbeit mit den MNOs....26
3.3.2 Bewegungs- und Zutrittsrechte für Einsatzpersonal....26
3.3.3 Notstromversorgung/NEAs 27
3.3.4 Bevölkerungsorientierte Optionen....28
3.4 Interdependenzen der Maßnahmen bzw. der Gestaltungsoptionen unter- bzw. zueinander 28
4 Ausblick 30
5 Anhang....31
Abkürzungsverzeichnis....32
Impressum....35

1 Einleitung

Mit diesem Dokument erfolgt die Fortschreibung des im Jahr 2022 von der Bundesnetzagentur veröffentlichten Strategiepapiers „Resilienz der Telekommunikationsnetze“, welches in enger und abgestimmter Zusammenarbeit mit dem Bundesministerium für Digitales und Staatsmodernisierung (BMDS) entstanden ist.

Die seinerzeit beschriebenen Szenarien wurden vor dem Hintergrund der Entwicklungen seit 2022 erneut betrachtet, hinsichtlich ihrer möglichen Auswirkungen bewertet und an die aktuellen Rahmenbedingungen angepasst.

Anlässe waren insbesondere die beiden Infrastrukturangriffe in Berlin im September 2025 und Januar 2026, die in die Betrachtung mit einbezogen wurden. Im September 2025 führte ein Brandanschlag auf zwei Strommasten im Berliner Südosten zu einem großflächigen Stromausfall, von dem zeitweise rund 50.000 Haushalte und etwa 2.000 Gewerbebetriebe betroffen waren.[1] Anfang Januar 2026 verursachte ein Brand an einer Kabelbrücke über den Teltowkanal im Berliner Südwesten einen weiteren großflächigen Stromausfall. Dabei waren rund 45.000 Haushalte und 2.200 Gewerbekunden betroffen; die vollständige Wiederherstellung der Stromversorgung dauerte rund 100 Stunden.[2] [3] Die Vorfälle haben illustriert, dass Resilienz nicht isoliert im Telekommunikationsbereich (TK-Bereich) betrachtet werden kann und die Verfügbarkeit der TK-Netze maßgeblich von einer zuverlässigen Energieversorgung abhängt. Die Fortschreibung erfolgte in engem fachlichem Austausch mit dem BMDS und unter Einbeziehung unterschiedlicher Ressorts der Bundesländer sowie der vier Mobilfunknetzbetreiber (MNOs) Deutsche Telekom, Telefónica Germany, Vodafone und 1&1 AG.

Zur Abstimmung des finalen Ergebnisses dieses Strategiepapiers wurden durch Konsultation weitere Stakeholder eingebunden. Diese sind am Ende dieses Strategiepapiers in Kapitel 5 gelistet.

Ziel des Strategiepapiers ist es, einen praxisorientierten Überblick zu geben, welche TK-bezogenen Maßnahmen bzw. darüberhinausgehenden Gestaltungsoptionen in anderen Bereichen zukünftig zu einer Steigerung der Resilienz der Telekommunikation beitragen können. Es soll dabei unterstützen, bestehende Risiken und Abhängigkeiten zu bewerten sowie die Widerstandsfähigkeit zu erhöhen.

Adressaten des Strategiepapiers sind die Betreiber von TK-Netzen und die Anbieter von TK-Diensten, wobei die zuvor benannten MNOs im Fokus stehen, da sie im Betrachtungsrahmen für relevante Bestandteile der TK-Infrastruktur in Deutschland verantwortlich sind. Ihnen kommt besondere Bedeutung zu, da sie die Verantwortung tragen, die Abhängigkeiten ihrer Netze zu analysieren und geeignete Maßnahmen zur Aufrechterhaltung bzw. Wiederherstellung der Kommunikationsfähigkeit zu treffen.

Darüber hinaus werden im Papier auch TK-bezogene Maßnahmen beschrieben, welche nicht unmittelbar in der bestehenden Infrastruktur umgesetzt werden können bzw. sollen. Das Strategiepapier dient damit als

---

[1] Vgl. https://www.stromnetz.berlin/fur-berlin/johannisthal/, abgerufen am 20.10.2026

[2] Vgl. https://www.stromnetz.berlin/uber-uns/presse/pressemitteilungen-2026/nach-brand-an-kabelbruecke-stromausfall-im-suedwesten-berlins/, abgerufen am 20.10.2026

[3] Vgl. https://www.stromnetz.berlin/uber-uns/presse/pressemitteilungen-2026/strom-ist-fur-alle-wieder-da/, abgerufen am 20.10.2026

Orientierung für die Weiterentwicklung der Resilienz im TK-Bereich, entfaltet aber keine rechtlich bindende Wirkung bzw. enthält keine über die gesetzlich bestehenden Vorgaben hinausgehenden Verpflichtungen. Entsprechende regulatorische Vorgaben finden sich in den §§ 165 und 185 TKG sowie im Katalog von Sicherheitsanforderungen (§ 167 TKG).

Angestrebt wurde bis Ende Oktober 2026 eine aufdatierte Version des bestehenden Strategiepapiers „Resilienz der TK-Netze“ aus dem Jahr 2022. Dabei sollten in diesem ersten Schritt lediglich die mittlerweile stabilisierten Erkenntnisse aus den Vorfällen in Berlin im September 2025 bzw. im Januar 2026 aufgenommen werden („Version 1.9“). Struktur und Aufbau der neuen Version (V1.9) orientieren sich an der ersten Version des Strategiepapiers.

In einem weiteren Schritt ist nach dieser Ergebnissicherung vorgesehen, nach Oktober 2026 sukzessive weitere Szenarien zu analysieren und in das Strategiepapier aufzunehmen. Dabei sollen auch die Erfahrungen anderer Mitgliedstaaten mit der Umsetzung von Maßnahmen zur Steigerung der Sicherheit und Resilienz der TK-Netze ausgewertet und berücksichtigt werden. Dies wird in enger inhaltlicher Abstimmung zwischen Bund und Ländern erfolgen. Dazu sollen eine gemeinsame Plattform sowie geeignete Austauschformate etabliert werden. Bereits erkennbare Szenarien werden jedoch schon jetzt zumindest als Gliederungspunkte in die vorliegende Version mit aufgenommen.

Die Bundesnetzagentur formuliert in der Fortschreibung Maßnahmenempfehlungen für die TK-Branche auf Basis eines Bottom-Up-Ansatzes. Hierbei liegt der Fokus auf dem Szenario der Störung der Energieversorgung. Dazu werden TK-bezogene Maßnahmen aufgeführt, welche die Resilienz der TK-Netze und damit die Verfügbarkeit von TK-Diensten auch bei länger andauernden Stromausfällen verbessern. Das Strategiepapier richtet sich also an die TK-Unternehmen, insbesondere die Betreiber des öffentlichen Mobilfunks.

Neben dieser generischen Stärkung der Resilienz der TK-Netze, die automatisch auch die Resilienz des Notrufs erhöhen würde, könnten auch spezifische Maßnahmen zur Stärkung des Notrufs allein diskutiert werden. Für diese sieht das Telekommunikationsgesetz (TKG) in § 164 jedoch spezifische Verfahren mit vorgeschriebenen Beteiligungsrechten vor, so dass in dieses Strategiepapier zur Resilienz der TK-Netze lediglich eine deklaratorische Beschreibung der Rechtslage und möglicher Lösungsansätze aufgenommen werden kann.

Zusätzlich werden Handlungsoptionen aufgezeigt, die organisatorischer Natur sind und länderseitige Möglichkeiten darstellen, wie Abläufe und Strukturen des Krisenmanagements gestaltet werden können. Die Benennung als „Gestaltungsoptionen“ weist bereits aus, dass es hierbei nicht um verbindliche Vorgaben gehen kann.

Zudem wird aufgezeigt, welche Maßnahmen bzw. Gestaltungsoptionen Interdependenzen unter- bzw. zueinander haben. Schnittstellen zwischen TK-bezogenen Maßnahmen und organisatorischen Gestaltungsoptionen werden ggf. deutlich gemacht.

2 Beschreibung der betrachteten Szenarien

Zur Fortschreibung des Strategiepapiers wurden die Szenarien aus dem „Strategiepapier Resilienz der Telekommunikationsnetze“ aus dem Jahr 2022 herangezogen und insbesondere vor dem Hintergrund der Infrastrukturanschläge im September 2025 und Januar 2026 in Berlin erneut überarbeitet und an die aktuellen Rahmenbedingungen angepasst. Dabei spielten auch geopolitische Spannungen und andere hybride Bedrohungslagen eine Rolle.

Einleitend werden die Szenarien skizziert. Außerdem werden die Auswirkungen der einzelnen Szenarien, insbesondere auf die Verfügbarkeit der Telekommunikation, soweit identifizierbar dargestellt. Es folgt eine Bewertung der Szenarien, bei der soweit möglich auch eine Einschätzung darüber erfolgt, in welcher Häufigkeit und Breite das jeweils betrachtete Szenario eintreten kann. Als Abschluss dieses Kapitels werden die Interdependenzen aller Szenarien zusammenfassend betrachtet und beschrieben, da eine isolierte Betrachtung einzelner Szenarien nicht in allen Konstellationen ausreichend wäre.

2.1 Störung der Energieversorgung

2.1.1 Beschreibung des Szenarios

Die Verfügbarkeit von TK-Netzen und -diensten ist in hohem Maße von einer zuverlässigen Energieversorgung abhängig. Daher ist ein relevantes, zu betrachtendes Szenario der Ausfall ebendieser, was z.B. durch technische Defekte, Wetterereignisse, Anlagenschäden oder Angriffe auf die diesbezügliche Infrastruktur verursacht werden kann. Dabei kann eine Störung der Energieversorgung danach unterschieden werden, ob diese vollständig ausfällt oder eine eingeschränkte bzw. instabile Energieversorgung vorliegt.

2.1.2 Auswirkungen des Szenarios

Aufgrund der beschriebenen Abhängigkeit der TK-Netze und -dienste von einer funktionierenden Energieversorgung würden diese bei einer Störung der Energieversorgung nicht funktionieren, falls die TK-Einrichtungen über keine geeignete Notstromversorgung verfügen. Eine solche Störung kann sich dabei sowohl auf einzelne TK-Standorte oder Teilnetze als auch auf größere regionale oder überregionale Bereiche auswirken.

Die Auswirkungen einer Energieversorgungsstörung auf TK-Netze hängen wesentlich von deren räumlicher Ausdehnung und Dauer sowie von der Kritikalität der betroffenen Netzelemente ab. Während großflächige und langanhaltende Energieausfälle eine besondere Herausforderung für die Aufrechterhaltung von TK-Diensten darstellen, können auch lokal begrenzte Ereignisse erhebliche Auswirkungen haben, wenn zentrale Standorte, wichtige Netzknoten oder besonders relevante Versorgungsbereiche betroffen sind.

Kritische Faktoren können dabei insbesondere sein:

- die begrenzte Verfügbarkeit gespeicherter Energiereserven,
- die Nachversorgung mit Energieträgern für Notstromsysteme,
- die Erreichbarkeit und Zugänglichkeit betroffener Standorte,
- die Verfügbarkeit von Personal, Dienstleistern und Ersatzkomponenten,
- die Dauer der Wiederherstellung der Energieversorgung,

- der Zeitablauf bis zur Erlangung einer stabilen Informationslage,
- die evtl. notwendige Koordinierung mit Nachbarstaaten.

Bei länger andauernden oder großflächigen Energieversorgungsstörungen können TK-Netzbetreiber zudem mit anderen kritischen Bedarfsträgern, beispielsweise Einrichtungen des Gesundheitswesens, Sicherheitsbehörden, Katastrophenschutzorganisationen oder Betreibern weiterer kritischer Infrastrukturen, um begrenzte Ressourcen konkurrieren, falls dies nicht durch vorsorgliche technische und organisatorische Maßnahmen verhindert wird. Eine sektorübergreifende Abstimmung und Priorisierung gewinnt daher insbesondere bei umfangreichen Schadenslagen an Bedeutung.

Neben der Energieversorgung der Netzinfrastruktur ist auch die Versorgung der Endgeräte zu berücksichtigen. Teilnehmerseitige TK-Geräte, insbesondere stationäre Endgeräte und Router, fallen bei einem Ausfall der Stromversorgung in der Regel unmittelbar aus. Mobile Endgeräte können abhängig vom Ladezustand für einen begrenzten Zeitraum weiter genutzt werden. Für mobile Endgeräte stehen oftmals alternative Lademöglichkeiten wie Powerbanks oder Kraftfahrzeuge zur Verfügung. Ihre Kommunikationsfähigkeit ist jedoch von der weiteren Verfügbarkeit der Mobilfunknetze sowie deren Energieversorgung und Auslastung abhängig.

2.1.3 Bewertung des Szenarios

Für die Bewertung der Resilienz von TK-Netzen ist daher nicht allein die Dauer einer Energieversorgungsstörung entscheidend. Maßgeblich ist vielmehr das Zusammenwirken verschiedener Faktoren:

- vorhandene Redundanzen,
- alternative Versorgungsmöglichkeiten und
- die Fähigkeit zur Priorisierung und Wiederherstellung kritischer Kommunikationsdienste.

Dabei spielen auch bestimmte statistische Ausfallwahrscheinlichkeiten zur Dauer und Wirkungsbreite eines möglichen Stromausfalls eine Rolle wie z.B. die räumliche Ausdehnung der Störung, Anzahl und Bedeutung betroffener Standorte oder die Abhängigkeit anderer kritischer Infrastrukturen.

Die durchschnittliche Versorgungsunterbrechung je angeschlossenen Letztverbraucher innerhalb eines Kalenderjahres in Deutschland betrug 11,68 Minuten im Jahr 2024 (Bundesweite Kennzahlenentwicklung Strom, Stand: 09.10.2025). Allerdings sagt der Durchschnitt als Kennzahl (hier in Minuten) mehr über die Eintrittswahrscheinlichkeit als über das Ausmaß der Betroffenheit im Einzelfall aus.

2.2 Naturkatastrophen

2.2.1 Beschreibung des Szenarios

Ein weiteres zentrales Szenario stellen Naturkatastrophen dar, die als starke und ungewöhnliche Naturereignisse beschrieben werden können und verheerende Schäden anrichten können. Beispiele, wie sich Naturkatastrophen äußern, sind u.a. Überschwemmungen, Orkane, Erdbeben oder Vulkanausbrüche, die z.B. durch Plattenverschiebungen oder klimatische Veränderungen ausgelöst werden.

2.2.2 Auswirkungen des Szenarios

Naturkatastrophen oder außergewöhnliche klimatische Bedingungen mit Wirkung auf die Rechenzentren und auf Technikstandorte, in denen Leit- und Steuersysteme betrieben werden, sowie die Leitungen zwischen ihnen, können zu einer Störung der Steuerbarkeit der TK-Netze führen. Dies bringt eine verringerte Leistungsfähigkeit, eingeschränkte Steuerbarkeit oder den Ausfall von TK-Netzen mit sich.

Nach schwerwiegenden Naturkatastrophen in Form von Überflutungen, wie z. B. bei der Flutkatastrophe im Ahrtal 2021, ist es häufig nicht möglich, Straßen und Zufahrtswege zur Wartung und Instandsetzung von Technikstandorten zu nutzen. Dies gestaltet, neben der möglicherweise notwendigen, aber ausbleibenden Instandsetzung, auch die Versorgung von physisch noch intakten Standorten mit Kraftstoff oder Notstromaggregaten als schwierig.

Große Hitzewellen können Rechenzentren durch überlastete Klimaanlagen in ihrer Leistungsfähigkeit derart einschränken, dass die angebotenen TK-Dienste nicht im notwendigen Umfang erbracht werden können. Dies kann in einer solchen Situation auch die Energieversorger und deren Netze sowie Steuerungen selbst betreffen, was zusätzlich zu einer temporären Energieunterversorgung und zum regionalen Netzausfall führen kann.

Dürreperioden können Kaskadeneffekte in der Stromversorgung auslösen und Kraftwerke in ihrer Leistung begrenzen, da häufig das Wasser der umliegenden Flüsse zur Kühlung der Kraftwerke verwendet wird. Durch Dürre oder Hitzegewitter hervorgerufene Brände können sich in der Fläche ausbreiten und Infrastrukturstandorte beschädigen sowie Zufahrtswege blockieren und somit Wartung, Reparatur sowie Notstromversorgung erschweren. Bei Blitzeinschlägen besteht zudem die Gefahr, dass elektromagnetische Störungen (LEMP) versursacht werden können und Infrastruktur beschädigt werden kann.

Auch Sonnenstürme stellen eine außergewöhnliche Gefahr für die Integrität und die Funktionsfähigkeit der TK-Netze dar. Je nach Intensität können Schäden an terrestrischen Einrichtungen und Satelliten hervorgerufen und beispielsweise sogar Unterseekabel über längere Zeiträume gestört werden.

2.2.3 Bewertung des Szenarios

Die Resilienz lässt sich vor dem Hintergrund des Szenarios der Naturkatastrophen maßgeblich dadurch beeinflussen, dass technische Redundanzen vorgehalten werden, für eine Notstromversorgung gesorgt ist und insgesamt eine angemessene Härtung der Infrastruktur besteht.

2.3 Wirtschaftliche Engpasssituationen

2.3.1 Beschreibung des Szenarios

Das Szenario beschreibt eine Situation, in der durch Störungen oder Ausfälle von Lieferketten, beispielsweise infolge von Mangellagen, für die Errichtung, den Erhalt und den Betrieb kritischer Infrastrukturen erforderliche Vorprodukte, Produkte und/oder Komponenten nicht oder nicht rechtzeitig zur Verfügung stehen.

2.3.2 Auswirkungen des Szenarios

Aufgrund gestörter Lieferketten kann mittelfristig es zu Mangellagen bei für den weiteren Ausbau der TK-Infrastruktur benötigten Komponenten kommen. Dies führt zu Verzögerungen bei geplanten Ausbauvorhaben und kann die weitere Entwicklung der TK-Infrastruktur beeinträchtigen.

Durch die fehlende Verfügbarkeit notwendiger Ersatzprodukte können vorgesehene Wartungs- und Instandhaltungszyklen nicht eingehalten werden. Dadurch erhöht sich die Ausfallwahrscheinlichkeit von Komponenten und technischen Einrichtungen, sodass Beeinträchtigungen oder Ausfälle von TK-Diensten drohen. Partielle Ausfälle zwingen den Datenverkehr auf verbleibende Trassen auszuweichen. Hieraus können Überbelastungen entstehen.

Mangellagen auf dem Öl- oder Gasmarkt können die Energieversorgung beeinträchtigen und damit Auswirkungen auf den Betrieb der TK-Infrastruktur haben. Einschränkungen oder Ausfälle im Energiesektor können insbesondere dann eine Beeinträchtigung oder einen Ausfall von TK-Diensten zur Folge haben, wenn keine ausreichende oder ausreichend lange verfügbare Ersatzstromversorgung gewährleistet werden kann.

2.3.3 Bewertung des Szenarios

Das beschriebene Szenario ist im Jahr 2026 insbesondere vor dem Hintergrund der andauernden Kriege in der Ukraine und dem Iran, von Zollstreitigkeiten und Lieferbeschränkungen als realistisch einzuschätzen. Diese Entwicklungen können die Verfügbarkeit von für die TK-Infrastruktur benötigten Vorprodukten, Produkten und/oder Komponenten beeinträchtigen und dadurch zu Verzögerungen bei deren Beschaffung führen.

2.4 Hybride Bedrohungslagen

2.4.1 Beschreibung des Szenarios

Hybride Bedrohungen richten sich gegen politische, gesellschaftliche und wirtschaftliche Strukturen mit dem Ziel, staatliche Handlungsfähigkeit einzuschränken, gesellschaftliche Spaltung zu fördern sowie Vertrauen in staatliche Institutionen und demokratische Prozesse zu beeinträchtigen. Hierzu nutzen staatliche oder staatlich unterstützte Akteure koordinierte Kampagnen, in denen unterschiedliche Instrumente wie Desinformation, Cyberangriffe, Spionage, wirtschaftliche Einflussnahme sowie physische Sabotage Kritischer Infrastrukturen kombiniert eingesetzt werden. Hybride Aktivitäten umfassen dabei regelmäßig auch vorbereitende Maßnahmen zur Informationsgewinnung und Einflussnahme.

2.4.2 Auswirkungen des Szenarios

Im Kontext der TK-Resilienz sind insbesondere koordinierte Angriffe auf TK- und Energieinfrastrukturen von Bedeutung. Diese können sowohl Cyberangriffe als auch physische Sabotagehandlungen umfassen und erhebliche Beeinträchtigungen der TK-Versorgung verursachen. Zu den möglichen Folgen zählen Ausfälle oder Einschränkungen von Mobilfunk-, Internet- und Datennetzen, Beeinträchtigungen von Notruf-, Warn- und Informationssystemen sowie Einschränkungen der behördlichen Krisenkommunikation.

Aufgrund der engen Abhängigkeiten zwischen TK- und Energieinfrastrukturen können darüber hinaus sektorübergreifende Kaskadeneffekte entstehen, die weitere Kritische Infrastrukturen, die öffentliche Verwaltung, die Daseinsvorsorge sowie das gesellschaftliche Leben erheblich beeinträchtigen.

2.4.3 Bewertung des Szenarios

Spätestens seit dem russischen Angriffskrieg gegen die Ukraine ist die Eintrittswahrscheinlichkeit dieses Szenarios stark gestiegen und auf sehr hohem Niveau. Fast tägliche Meldungen in den öffentlichen Medien bestätigen, dass es eine enorme Vielzahl von hybriden Angriffen auf die Infrastruktur in Deutschland und Europa gibt.

Die Gefahren, die von diesem Szenario ausgehen, sind sehr vielfältig und haben je nach Ausprägung ein sehr hohes Gefährdungspotenzial auf wichtige Infrastruktur wie etwa die Energieversorgung, TK-Versorgung oder den Logistiksektor. Zudem können erfolgreiche Angriffe, wie die Brandanschläge in Berlin Adlershof und Berlin Steglitz, das Vertrauen der Bevölkerung in die staatlichen Strukturen und die freiheitliche demokratische Grundordnung untergraben.

Hybride Angriffe können von staatlichen, staatsnahen oder nichtstaatlichen Akteuren ausgehen. Die Bewertung sollte deshalb unabhängig vom Akteur auf Fähigkeiten, Motivation, Angriffspfade und mögliche Kaskadeneffekte abstellen.

2.5 Unruhen

2.5.1 Beschreibung des Szenarios

Unruhen zeichnen sich dadurch aus, dass sie durch einen Teil der Bevölkerung ausgelöst werden, der in der Regel unzufrieden mit den staatlichen Institutionen und deren Handeln sind. Solche Unruhen äußern sich in großen Protestaktionen, Ausschreitungen und im schlimmsten Fall Plünderungen und gewaltsamen Auseinandersetzungen.

Die Ursachen für das Entstehen von Unruhen sind häufig soziale Ungleichheiten, die - durch wirtschaftliche Krisen verstärkt - zutage treten. Dabei kann es zu einem Vertrauensverlust gegenüber den staatlichen Institutionen und den politischen Entscheidungsträgern kommen.

Unruhen können aber auch durch staatliche Akteure verursacht werden, indem gezielt versucht wird, durch teleologische und hybride Kriegsführung gezielte Einflussnahme auf die Zufriedenheit der Bevölkerung eines Ziellandes auszuüben.[4]

2.5.2 Auswirkungen des Szenarios

Die Auswirkungen dieses Szenarios sind sehr vielfältig. Die Unruhen können sich in friedlichen Protesten bis zu schweren, gewaltsamen Auseinandersetzungen äußern.

Bei schweren Auseinandersetzungen ist denkbar, dass dabei neuralgische TK- oder Energieinfrastruktur beschädigt oder zerstört wird. Die Unruhen können auch als Tarnung für staatliche Akteure dienen, um gezielt Infrastruktur zu sabotieren, während die staatlichen Institutionen damit beschäftigt sind, die Unruhen und den damit einhergehenden Folgen einzudämmen.

---

[4] Vgl. https://metis.unibw.de/assets/pdf/metis-studie42-2024_12-rus_ostflanke.pdf, abgerufen am 20.08.2026

Gleichzeitig ist die Verfügbarkeit von Servicetechnikern eingeschränkt und es wird den verfügbaren Servicetechnikern der Infrastrukturunternehmen erschwert, den Zugang zu relevanter TK- oder Energieinfrastruktur zu erlangen, wenn diese sich in Gebieten des Ausnahmezustandes befinden und nicht der Kontrolle der staatlichen Sicherheitsorgane unterliegen.

Die Lieferketten und auch die Logistik, um beschädigte oder zerstörte TK-Infrastruktur zu reparieren oder zu ersetzen, wird durch blockierte Zuwegungen erschwert oder unmöglich.

Durch ein erhöhtes Anrufaufkommen in den Notrufabfragestellen oder der Bevölkerung untereinander, um Notrufe abzusetzen oder sich gegenseitig zu den Auswirkungen der Unruhen zu informieren, können die TK-Netze überlastet werden.

Eine mögliche Beeinträchtigung durch beschädigte Energieinfrastruktur können z. B. Netzengpässe darstellen, mit der Folge einer Beeinträchtigung der Energieversorgung, was den Ausfall von TK-Netzen zusätzlich begünstigt.

2.5.3 Bewertung des Szenarios

Die Eintrittswahrscheinlichkeit ist stark an gesellschaftliche, wirtschaftliche und politische Rahmenbedingungen gekoppelt. Wie bereits in der Beschreibung des Szenarios genannt, können wirtschaftliche Defizite als Brennglas dienen und somit gesellschaftliche und soziale Ungleichheiten multiplizieren.

Die Auswirkungen eines solchen Szenarios können regional begrenzt bleiben. Sollten jedoch Bevölkerungsschichten betroffen sein, die sich national oder auch international betroffen sehen, können sich Unruhen entsprechend weit ausdehnen. Als Beispiel kann die Ausbreitung des arabischen Frühlings auf eine ganze Region auf der arabischen Halbinsel dienen.

Auf der zeitlichen Ebene kann sich ein solches Szenario je nach Schweregrad über wenige Stunden bis mehrere Tage und Wochen ausdehnen. Es ist aber auch möglich, dass Unruhen in zeitlich nicht aneinanderhängenden Abständen immer wieder „aufflammen“.

Dieses Szenario hat große Wechselwirkungen mit den Szenarien wirtschaftlicher Engpässe und hybrider Bedrohungslagen. Unruhen können durch großangelegte Desinformationskampagnen begünstigt oder gar ausgelöst werden. Unruhen können auch durch staatliche Akteure verursacht werden, um in Vorbereitung einer kriegerischen Auseinandersetzung den jeweiligen Kriegsgegner zu paralysieren und die Handlungsfähigkeit des angegriffenen Lands sowohl zivil als auch militärisch einzuschränken.

2.6 Kriegerische Auseinandersetzungen

2.6.1 Beschreibung des Szenarios

Eine kriegerische Auseinandersetzung stellt TK-Netze vor außergewöhnliche Herausforderungen, da diese aufgrund ihrer strategischen Bedeutung zu unmittelbaren Zielen militärischer Angriffe werden können. In der Regel werden diese Angriffe flankiert durch gut vorbereitete hybride Angriffe auf alle neuralgischen Punkte einer Informationsgesellschaft.

Insbesondere zentrale Netzknoten, Kabeltrassen, Mobilfunkstandorte sowie Einrichtungen der Energieversorgung und Netzsteuerung können gezielt angegriffen oder sabotiert werden. Die Angriffsmittel können hierbei vielfältig sein (z.B. aus der Luft).

Neben offenen militärischen Angriffen sind auch verdeckte Sabotagehandlungen gegen besonders kritische und neuralgische Infrastrukturelemente möglich.

Darüber hinaus besteht im Falle des Einsatzes taktischer Nuklearwaffen die Gefahr großflächiger elektromagnetischer Auswirkungen (NEMP), durch die elektronischen Komponenten und Kommunikationssysteme erheblich beeinträchtigt oder zerstört werden können.

2.6.2 Auswirkungen des Szenarios

Die Auswirkungen eines solchen Szenarios können weit über unmittelbar beschädigte Netzelemente der TK-Netze hinausgehen. Auch benötigte Basisinfrastruktur, wie etwa Elemente des Stromnetzes, können durch großflächige Angriffe erheblich beeinträchtigt werden.

Der Ausfall oder die Beeinträchtigung kritischer TK-Infrastrukturen kann Kommunikations-, Führungs- und Koordinierungsstrukturen stören und damit die staatliche und gesellschaftliche Handlungsfähigkeit erheblich einschränken.

Gleichzeitig bestehen Abhängigkeiten zu weiteren kritischen Infrastrukturen, deren Betrieb auf eine zuverlässige TK-Versorgung angewiesen ist.

Dadurch können sich Störungen über verschiedene Sektoren hinweg fortsetzen und zu erheblichen Kaskadeneffekten führen.

Die verdeckte Durchführung von Sabotagehandlungen erschwert zudem deren frühzeitige Erkennung und eine zeitnahe Reaktion.

2.6.3 Bewertung des Szenarios

Insgesamt ist das Szenario als sehr hohes bis existenzielles Risiko für die Resilienz, Verfügbarkeit und Funktionsfähigkeit der TK-Infrastruktur zu bewerten. Die Eintrittswahrscheinlichkeit steigt in Deutschland mit zurzeit weltweit wachsenden geopolitischen Spannungen.

Das Schadenspotenzial wird insbesondere durch die strategische Bedeutung der TK-Netze, die mögliche Kombination unterschiedlicher Angriffsmethoden sowie die potenziell großflächigen und sektorübergreifenden Auswirkungen bestimmt.

Eine kriegerische Auseinandersetzung kann daher die Fähigkeit zur Aufrechterhaltung essenzieller Kommunikations- und Versorgungsleistungen und damit die Sicherheit der Bevölkerung erheblich beeinträchtigen.

Kriegerische Auseinandersetzungen werden in der Regel durch hybride Angriffe begleitet. Auch Desinformationskampagnen und durch staatliche Akteure ausgelöste Unruhen können eine kriegerische Auseinandersetzung flankieren, um dem Angreifer einen strategischen Vorteil zu verschaffen.

Der Steigerung von Robustheit, Redundanz, Wiederherstellungsfähigkeit und damit der Steigerung der allgemeinen Resilienz der TK-Netze kommt vor diesem Hintergrund eine herausragende strategische Bedeutung zu.

2.7 Fehlende Souveränität bei der Nutzung von IT- und TK-Technologie

2.7.1 Beschreibung des Szenarios

Die TK-Infrastruktur weist in weiten Bereichen eine Abhängigkeit von großen und marktmächtigen Unternehmen mit Sitz außerhalb Deutschlands und der Europäischen Union auf. Dies betrifft insbesondere Anbieter zentraler Komponenten, Systeme und Technologien, die für den Aufbau, die Weiterentwicklung und den Betrieb moderner TK-Netze von Bedeutung sind.

In einzelnen technologischen Schlüsselbereichen bestehen nur begrenzte europäische Einfluss- und Kontrollmöglichkeiten hinsichtlich der Entwicklung, Herstellung, Weiterentwicklung und Bereitstellung wesentlicher Komponenten und Technologien. Dies betrifft insbesondere Bereiche, in denen eine geringe Anzahl marktprägender Anbieter verfügbar ist und europäische Alternativen nur eingeschränkt bestehen.

Der Einsatz hochspezialisierter Technologien kann zu Abhängigkeiten von einzelnen Herstellern, Lieferketten oder technologischen Plattformen führen. Resilienzrelevante Risiken entstehen insbesondere dann, wenn wesentliche Funktionen nicht durch alternative Anbieter, interoperable Lösungen oder diversifizierte Lieferketten abgesichert werden können.

2.7.2 Auswirkungen des Szenarios

Der Einsatz von Komponenten, deren Quellcode nicht öffentlich einsehbar ist, begünstigt die Abhängigkeit von externen Herstellern und deren Technologien. Der Einsatz solcher Closed-Source-Komponenten schränkt die Möglichkeiten zur eigenständigen Analyse und Bewertung der technischen Eigenschaften der eingesetzten Systeme ein. Fehlt zusätzlich eine auf etablierten Prüf-, Zertifizierungs- und Auditverfahren beruhende Bewertung sicherheitsrelevanter Systeme ist eine Bewertung nahezu unmöglich.

Bei Komponenten, deren technische Implementierung nicht vollständig offengelegt ist, bestehen nur eingeschränkte Möglichkeiten zur unabhängigen Überprüfung der Funktionsweise sowie der zugrunde liegenden Sicherheitsmechanismen. Dies erschwert die Bewertung der Vertrauenswürdigkeit und Sicherheit eingesetzter Technologien.

Das Risiko einer Einflussnahme durch externe Akteure kann sich bei Abhängigkeit von externen Herstellern und Technologien erhöhen. Risiken können dort entstehen, wo erhebliche Abhängigkeiten von einzelnen Herstellern oder Lieferketten bestehen und keine ausreichenden Ausweich-, Austausch- oder Diversifizierungsmöglichkeiten vorhanden sind. Die Gefährdung durch korrumpierte Firmware-Updates kann zu Kettenreaktionen und Ausfällen kritischer Netzfunktionen führen.

Eine eingeschränkte Kontrolle über zentrale Komponenten und technologische Schlüsselbereiche gefährdet die Integrität der TK-Netze. Sicherheit und Integrität von TK-Netzen hängen maßgeblich von wirksamen Sicherheitsprozessen, kontinuierlichem Patchmanagement, technischer Überprüfung sowie regulatorischen Sicherheitsanforderungen ab.

Abhängigkeiten von einzelnen Herstellern und technologischen Lösungen können die Verfügbarkeit kritischer Netzfunktionen erschweren. Technische Störungen, Sicherheitsvorfälle oder Einschränkungen bei der Bereitstellung von Herstellerleistungen führen zu einer erhöhten Gefährdung der Netzverfügbarkeit und der zuverlässigen Erbringung von TK-Diensten.

2.7.3 Bewertung des Szenarios

Die bestehenden Abhängigkeiten von externen Herstellern und Technologien sind aufgrund ihrer möglichen Auswirkungen auf die Sicherheit und Verfügbarkeit kritischer TK-Infrastrukturen als hohes strategisches und sicherheitspolitisches Risiko zu bewerten. Insbesondere bei zentralen Komponenten und technologischen Schlüsselbereichen erschweren bestehende Abhängigkeiten die langfristige Wahrung von Handlungsfähigkeit und Einflussmöglichkeiten europäischer Akteure.

Die Abhängigkeit von außerhalb Deutschlands und der Europäischen Union ansässigen Unternehmen führt in bestimmten Bereichen zu eingeschränkten Kontroll- und Einflussmöglichkeiten über kritische TK-Infrastrukturen. Dies betreffen insbesondere die Entwicklung, Bereitstellung und technische Ausgestaltung wesentlicher Komponenten und Systeme.

Die Nutzung von Technologien und Komponenten externer Hersteller schafft potenzielle Ansatzpunkte für eine Einflussnahme durch externe Akteure. Insbesondere bei geopolitischen Spannungen besteht das Risiko, dass wirtschaftliche oder staatliche Interessen die Verfügbarkeit, Sicherheit oder Weiterentwicklung eingesetzter Technologien beeinflussen.

Bestehende technologische Abhängigkeiten beeinträchtigen die Resilienz und Vertrauenswürdigkeit der TK-Infrastruktur. Einschränkungen bei der Verfügbarkeit, Wartung oder Weiterentwicklung eingesetzter Komponenten können Auswirkungen auf die langfristige Versorgungssicherheit mit TK-Diensten haben.

Aus dem Szenario ergibt sich ein erhöhter Handlungsbedarf zur Stärkung der technologischen Souveränität und zur Verringerung einseitiger Abhängigkeiten. Wesentliche Handlungsfelder wären insbesondere die Diversifizierung von Lieferketten und Bezugsquellen sowie die verstärkte Nutzung überprüfbarer, sicherer und vertrauenswürdiger Netzkomponenten.

2.8 Menschliches Versagen

2.8.1 Beschreibung des Szenarios

Im laufenden Betrieb von TK-Netzen stellen menschliche Fehler ein erhebliches Betriebsrisiko dar. Dazu zählen Fehlkonfigurationen von Netzelementen, fehlerhafte Software-Updates, falsche Routing-Einträge oder das Abweichen von etablierten Betriebsprozessen.

Eine weitere Ursache menschlichen Versagens sind physische Beschädigungen von Netzelementen. Diese entstehen überwiegend im Rahmen von Tiefbau-, Instandhaltungs- oder Abrissarbeiten. Ein typisches Schadensbild ist das unbeabsichtigte Durchtrennen von Glasfaser- oder Kupfertrassen sowie die Beschädigung von Stromzuleitungen für Vermittlungsstellen oder Mobilfunkstandorte durch Bagger und Erdarbeiten.

2.8.2 Auswirkungen des Szenarios

Die Beschädigung von Glasfasertrassen oder hochrangigen Verbindungswegen führt zu einem unmittelbaren Ausfall großer Datenkapazitäten. In der Folge kommt es zu massiven Unterbrechungen im regionalen oder überregionalen Daten- und Sprachverkehr, wodurch ganze Gebiete von der digitalen Kommunikation abgeschnitten werden können.

Fallen durch Fehlhandlungen oder physische Einwirkungen zentrale Knotenpunkte wie Internet-Knoten (IXPs) oder Kernvermittlungsstellen aus, hat dies Auswirkungen auf das gesamte gesellschaftliche und wirtschaftliche Leben. Betroffen sind nicht nur private Haushalte, sondern auch die Handlungsfähigkeit von Behörden, Rettungsdiensten, Finanzinstituten und Unternehmen, was zu erheblichen wirtschaftlichen Schäden und Versorgungsengpässen führen kann.

Auch bei vorhandenen Redundanzsystemen können Beeinträchtigungen auftreten, wenn die Ausweichpfade durch mangelhafte Diversifizierung nicht ausreichend räumlich getrennt verlaufen. Ebenso können kurzfristig auftretende Überlastungen der Ausweichrouten oder zeitliche Verzögerungen bei Umschaltprozessen dazu führen, dass der Netzbetrieb trotz theoretischer Absicherung spürbar gestört wird.

2.8.3 Bewertung des Szenarios

Das Risiko menschlichen Versagens weist im Verglich zu anderen Bedrohungsszenarien eine sehr hohe Eintrittswahrscheinlichkeit auf. Sowohl unbeabsichtigte Konfigurationsfehler als auch Beschädigungen von Leitungsnetzen im Zuge von Bauarbeiten kommen kontinuierlich vor. Dies macht dieses Szenario zu einer dauerhaften und praktisch unvermeidbaren Herausforderung für die TK-Netzresilienz.

Die Schwere der tatsächlichen Auswirkungen variiert erheblich und wird maßgeblich von der Netzarchitektur bestimmt. Eine starke räumliche Bündelung von Trassen, mangelnde Wegediversität oder eine hohe Konzentration von Datenverkehr auf einzelne zentrale Netzknoten erhöhen die Auswirkungen des Schadens im Ereignisfall um ein Vielfaches bis hin zu weiträumigen Systemausfällen.

Besonders kritisch wird das Szenario bewertet, wenn Fehler an zentralen TK-Netzkomponenten auftreten oder wenn Ausweichpfade nicht rechtzeitig oder gar nicht zur Verfügung stehen.

2.9 Pandemien

2.9.1 Beschreibung des Szenarios

Eine Pandemie zeichnet sich durch die großflächige, grenzüberschreitende Ausbreitung eines Erregers aus, welche zu umfassenden globalen sowie nationalen Einschränkungen des öffentlichen Lebens führt. Zur Eindämmung des Infektionsgeschehens werden Staaten und Behörden zur Umsetzung weitreichender Maßnahmen zur Kontaktreduzierung gezwungen, wodurch die gewohnten Abläufe im gesellschaftlichen und wirtschaftlichen Leben drastisch verändert und entschleunigt werden.

Parallel dazu zeichnet sich das Szenario durch extrem hohe Krankenstände in der gesamten Bevölkerung aus. Dies kann von strengen behördlichen Vorgaben wie Ausgangssperren oder die vollständige Abriegelung ganzer Städte oder Regionen begleitet werden. Dadurch werden sowohl die personelle Verfügbarkeit als auch die Mobilität im gesamten öffentlichen Raum stark eingeschränkt.

2.9.2 Auswirkungen des Szenarios

Durch die die weitreichenden Einschränkungen und personellen Ausfälle gerät die Gesamtwirtschaft ins Stocken. Produktionsstätten stehen vielerorts still und bestehende Logistikketten werden unterbrochen, da Transportwege blockiert sind oder nötiges Personal für den Güterverkehr fehlt.

Aus diesen Produktionsstillständen und gestörten Lieferketten können gravierende Engpässe bei der Hardware- und Kraftstoffversorgung resultieren. Ersatzteile für technische Anlagen sowie Kraftstoffe für Fahrzeuge und Notstromaggregate stehen dadurch nur noch eigeschränkt zur Verfügung. Die Einsatzfähigkeit erforderlicher System- oder Servicetechniker kann ebenfalls stark eingeschränkt sein.

Als Folge der eingeschränkten Material- und Personalsituation sowie veränderter Auslastungsmuster ist eine temporäre Reduzierung der Leistungsfähigkeit und Verfügbarkeit der TK-Netze möglich. Wartungs- und Instandhaltungsarbeiten können nicht mehr in gewohnter Geschwindigkeit durchgeführt werden, was die Stabilität der Dienste stellenweise beeinträchtigen kann.

Gleichzeitig entsteht eine massiv erhöhte Nachfrage nach digitalen Kommunikationsdiensten, da gesellschaftliche und wirtschaftliche Aktivitäten großflächig ins Homeoffice sowie in den virtuellen Raum verlagert werden. Dies führt zu einer dauerhaft hohen Grundlast im Daten- und Sprachverkehr der TK-Infrastruktur.

2.9.3 Bewertung des Szenarios

Dem Szenario wird eine mäßig hohe Eintrittswahrscheinlichkeit zugeschrieben. Obwohl weltweite Pandemien seltene Ereignisse sind, stellen globale Verflechtungen sowie neuartige Erreger ein reales und dauerhaft einzukalkulierendes Risiko dar. Dies hat die Corona-Pandemie gezeigt.

Das Szenario weist eine gute Beherrschbarkeit auf, sofern entsprechende Notfall- und Kontinuitätspläne bereits im Vorfeld detailliert definiert und etabliert sind. Durch präventive Maßnahmen, wie klare Vertretungsregelungen, erweiterte Remote-Zugriffe für die Netzsteuerung und vorbereitete Prozesse zur Priorisierung kritischer Dienste, lassen sich die operativen Betriebsabläufe auch unter erschwerten Bedingungen weitgehend stabil halten.

Kritisch wird die Lage jedoch, wenn Pandemiewirkungen mit zeitgleichen Störungen, wie bspw. großflächigen Stromausfällen oder gezielten Cyber-Angriffen, zusammenfallen oder es an logistischer Resilienz fehlt. Unterbrechen Lieferketten die Notstrom- und Ersatzteilversorgung dauerhaft oder fallen Schlüsselpersonen ersatzlos aus, kann die Handlungsfähigkeit der Netzbetreiber rasch an ihre Grenzen stoßen.

2.10 Interdependenzen der Auswirkungen aller Szenarien

Da einzelne Szenarien in einem engen oder auch weiter gefassten Zusammenhang stehen können, reicht eine isolierte Betrachtung einzelner Szenarien alleine nicht aus.

- Beispielsweise kann ein hybrider Angriff auf Komponenten der Strominfrastruktur einen Stromausfall auslösen und eine Störung der TK-Infrastruktur hervorrufen.
    - Die betroffenen TK-Unternehmen müssen sich also in den Maßnahmen nicht nur auf Ausfälle der eigenen TK-Infrastruktur vorbereiten,

    - sondern ggfs. auch Maßnahmen ergreifen, um die Verfügbarkeit der notwendigen Vorprodukte (Strom) in dem ihnen möglichen Rahmen unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit sicherzustellen.

- Der hybride Angriff kann durch die Angreifenden jedoch auch weiter genutzt werden, um Unruhen zu verursachen oder kriegerische Auseinandersetzungen vorzubereiten.
    - Die Maßnahmen, die in einem solchen Fall zu ergreifen wären, gehen weit über das Maß hinaus, was bei einem Stromausfall zu tun wäre.
- Möglicherweise kann ein hybrider Angriff auf die Strominfrastruktur zunächst auch als isoliertes, lokales Ereignis erscheinen, während jedoch auf dem gesamten Bundesgebiet viele dieser lokalen Ereignisse sich kumulieren und zu einem Großschadensereignis und einem großflächigen Stromausfall führen.
    - Hier erscheint es sinnvoll, diese lokalen Ereignisse in einem Zusammenhang betrachten zu können, um auf die drohende oder heranwachsende Gefahr eines Großschadensereignisses rechtzeitig vorbereitet zu sein.

Daraus lässt sich schließen, dass die Palette der zu ergreifenden Maßnahmen, um einen Ausfall der TK-Infrastruktur zu verhindern, sich mit voranschreiten der Breite und Tiefe der gewählten Szenarien erhöht. Diese Betrachtung gilt auch äquivalent für die Bandbreite der zu ergreifenden Maßnahmen, um den Wiederanlauf von zerstörter oder nicht verfügbarer TK-Infrastruktur zu bewältigen.

Diese zwar in einzelnen Szenarien differenzierte, jedoch im Zusammenhang geführte Betrachtungsweise hat den Vorteil, die Verhältnismäßigkeit der erforderlichen Maßnahmen genauer einzuschätzen, um die Folgen eines Szenarios oder mehrerer Szenarien nach Möglichkeit bewältigen zu können. Als Beispiel sei die Härtung einzelner Standorte gegen einen EMP/NEMP genannt, welche ein viel tiefer greifendes Erfordernis darstellt, als die Härtung gegen einen vorübergehenden Stromausfall.

Es ist auch kein Szenario erkennbar, welches das Schadenspotenzial aller anderen Szenarien von vornherein vollständig überdeckt. Das bedeutet, dass die zu ergreifenden Maßnahmen je nach Szenario, das es zu bewältigen gilt, angepasst werden müssen.

Darüber hinaus ist auch kein Szenario erkennbar, zu dessen Behebung Maßnahmen erforderlich wären, die im Widerspruch zu Maßnahmen stünden, die zur Behebung eines anderen Szenarios erforderlich wären.

3 Ableitung resilienzsteigernder Maßnahmen bzw. Gestaltungsoptionen

3.1 TK-bezogene Maßnahmen

Die im vorangegangenen Kapitel dargestellten Szenarien können Auswirkungen u. a. in personeller, logistischer bzw. technischer Hinsicht haben. Viele der potenziellen Auswirkungen werden bereits in Festlegungen nach dem TKG (z. B. im Sicherheitskatalog) adressiert.

In der nunmehr erfolgenden Auswertung der Großschadensereignisse in Berlin der Jahre 2025 und 2026 wird zunächst das Augenmerk auf die technische Ausrichtung von TK-Netzen gelegt. Ob und inwieweit sich aus diesen technischen Maßnahmen auch Anpassungsbedarf des rechtlichen Rahmens (z. B. Sicherheitskanon) ergeben könnte, ist nicht Gegenstand des Strategiepapiers.

Soweit nicht anders vermerkt, werden Maßnahmen beschrieben, die von den TK-Netzbetreibern oder zumindest im Zusammenspiel mit ihnen umgesetzt werden sollen.

Wann immer in den nachfolgenden Ausführungen der Begriff „betreiberübergreifend“ verwendet wird, erfolgt dies unter dem Gesichtspunkt der wirtschaftlich potenziell effizientesten Vorgehensweise. Maßgeblich ist dabei die Annahme, dass eine entsprechende Bündelung bzw. Abstimmung zwischen den beteiligten Betreibern in technischer Hinsicht zu einer möglichst effizienten Gesamtlösung führen kann. Sollte ein betreiberübergreifender Ansatz technisch, wirtschaftlich und/oder rechtlich nicht umsetzbar sein, gelten die genannten Überlegungen grundsätzlich entsprechend für eine geeignete Projektion auf einzelne Betreiber (bzw. auf einen stellvertretenden Betreiber). Eine diesbezügliche Vorfestlegung wird nicht getroffen.

Aus dem vorliegenden Strategiepapier erwachsen keinerlei unmittelbaren Verpflichtungen, ungeachtet ggf. gewählter stringenter Formulierungen. Solche sind in jedem Fall auf dem gesetzlich vorgesehenen Weg und unter Beachtung der rechtsstaatlichen Grundsätze festzulegen und nicht im Wege der Niederlegung strategischer Ansätze. Demgegenüber ist jedoch eine möglichst enge Zusammenarbeit mit den betreffenden TK-Unternehmen hinsichtlich der Gestaltung und Umsetzung Gewinn bringender Überlegungen anzustreben.

3.1.1 Grundsicherung der Kommunikationsfähigkeit in Krisensituationen

Die bisherigen Rahmenbedingungen und Einrichtungen für die gesetzlich gebotene Aufrechterhaltung von öffentlich zugänglichen Telekommunikationsdiensten sowie des Betriebs öffentlicher Telekommunikationsnetze sollen im Sinne der gesetzlichen Zielsetzung möglichst umfassend optimiert werden. Insbesondere soll für Mobilfunkteilnehmer in Krisensituationen, in denen die Aufrechterhaltung der Kommunikationsfähigkeit besonders relevant ist, eine Grundsicherung bereitgehalten oder zumindest schnellstmöglich wiederhergestellt werden. Unter dieser Grundsicherung wird die verlässliche Verfügbarkeit von Basisdiensten (Sprach- und Notruftelefonie sowie SMS-Dienste) zur Sicherung der Mindestkommunikation verstanden.

Sowohl Anbieter öffentlich zugänglicher Telekommunikationsdienste (mit mehr als 100.000 Vertragspartnern) als auch Betreiber öffentlicher Telekommunikationsnetze haben unmittelbar aus dem Gesetz Verpflichtungen. Weitere konkretisierende Maßgaben zur Umsetzung hat der Gesetzgeber nicht getroffen. Vor diesem Hintergrund könnte ein Potenzial zur Steigerung von Effektivität und Effizienz darin

liegen, die erforderliche Infrastruktur und Einrichtungen - wo immer rechtlich und technisch möglich - nicht anbieter- bzw. betreiberscharf abzugrenzen.

Die nachfolgenden Ausführungen in diesem Abschnitt sind hinsichtlich des tatsächlich mit ihnen verbundenem Verbesserungspotentials, ihrer rechtlichen und technischen Umsetzbarkeit, ihrer konkreten Ausgestaltung und unter dem Gesichtspunkt der Verhältnismäßigkeit zu diskutieren.

Vor diesem Hintergrund erscheint zunächst die Erstellung einer übergreifenden Übersicht hilfreich, aus der hervorgeht, mit welchen Infrastrukturelementen eine TK-Grundversorgung im Mobilfunk in Krisensituation mittels eines so genannten "Rumpfnetzes" möglich wäre, um die Telekommunikationssicherstellungspflicht resilienter auszugestalten. Hierbei würde es sich bei dem Rumpfnetz nach heutiger Erwartung nicht um eine eigenständig zu errichtende Infrastruktur handeln; vielmehr würde dieses eine für den Krisenfall noch zu konkretisierende Teilmenge der bereits bestehenden Netzkomponenten aus dem regulären Vollausbau abbilden. Dies könnte in einem noch zu diskutierenden Umfang Informationen zu vorhandenen Basisstationen einschließlich ihrer technischen Ausstattung und Parameter (Kataster) umfassen, insbesondere hinsichtlich Ausleuchtung, Notstromversorgung, Funktechnologie, Frequenzzuordnung sowie Anbindung an das Kernnetz, um eine belastbare Entscheidungs- und Planungsgrundlage zu schaffen im Sinne einer Art „Asset Management“).

Auf der Grundlage der Erfahrungen aus betrachteten Krisensituationen können evtl. folgende Kriterien für die Zuordnung einer Basisstation zum Rumpfnetz eine Rolle spielen:

- insbesondere ihre hierarchische Einordnung in der Netztopologie,
- die technische Kompatibilität und damit Kombinierbarkeit der Basisstationen aller Mobilfunknetzbetreiber untereinander,
- ihre potenzielle Reichweite zur Abdeckung größerer Flächen mit vergleichsweise geringer Anzahl von weiteren Basisstationen,
- die von ihr versorgten Privathaushalte oder Unternehmensstandorte sowie
- ihre Zuordnung zu Notfalleinrichtungen und deren Versorgung (insbesondere Leitstellen, Führungsstellen, Feuer- und Rettungswachen, Krankenhäuser sowie kritische Versorgungsinfrastrukturen).
- Ergänzend sind die jeweiligen örtlichen Versorgungsbedarfe und die Einsatzrelevanz in Krisenszenarien zu berücksichtigen.
- Weitere Aspekte können sein: Standortzugänglichkeit, Redundanz der Stromversorgung durch den Energieversorger, bauliche Verhältnisse für Notstromversorgung oder logistische Erreichbarkeit.

Basisstationen, die dem Rumpfnetz zugeordnet würden, könnten bevorzugt gehärtet und beim Wiederanlauf nach einem Havariefall bevorzugt werden, etwa durch den vorrangigen Einsatz entsprechender Notstromversorgungen sowie gegebenenfalls durch zusätzliche Netzersatzanlagen zur Sicherstellung der Funktionsfähigkeit.

Denkbar ist grundsätzlich auch, dass sich eine etwaige Nutzung fremder Netze in Katastrophenszenarien (Disaster Roaming) an bereits bestehenden Anforderungen und deren Umsetzung zum Notruf orientieren

könnte. Die Notrufmöglichkeiten über Mobilfunknetze sind im Sinne eines „Limited Service Access“ (LSA) schon heute und auf gesetzlicher Grundlage so auszugestalten, dass Notrufe auch über Fremdnetze abgesetzt werden können.

Die Zusammenführung und Auswertung von Informationen aus den Verantwortungsbereichen der einzelnen Betreiber ist so vorzunehmen, dass eine kartellrechtlich abgesicherte Vorgehensweise gewährleistet ist und etwaige wettbewerbsrechtliche Risiken durch geeignete technische, rechtliche und organisatorische Maßnahmen ausgeschlossen werden. Aus diesem Grund sind Rechtsgrundlage, Zweckbindung, Datenminimierung, Schutzbedarf (inklusive Betriebs- und Geschäftsgeheimnisse der Wettbewerber untereinander), Zugriffsberechtigung, Protokollierung, Aufbewahrung, Haftung, Finanzierung sowie geheimnisschutzrechtliche Anforderungen vorab verbindlich festzulegen.

Mit Blick auf den zeitlichen Verlauf muss auch diskutiert werden, ob und wie Design, Bau und Betrieb eines solchen Netzes möglich wären, da sich die Mobilfunknetze stetig weiterentwickeln und sich das "Rumpfnetz" jeder Änderung in den Mobilfunknetzen dynamisch anpassen müsste.

Ergänzend sollte hier auch einbezogen werden, welche weiteren Ansätze zur Grundsicherung der Kommunikationsfähigkeit in Krisensituationen alternativ und/oder ergänzend zum öffentlichen Mobilfunk geeignet sein könnten, z.B. öffentliches WLAN an einer zentralen Anlaufstelle mit Satellitenanbindung.

Initiative und Moderation liegen bei der Bundesnetzagentur, die damit den prozessualen Rahmen für die Erarbeitung, Abstimmung und Umsetzung der genannten Maßnahmen koordiniert. Hierzu wird erneut ein enger, fachlicher Austausch mit den MNOs und den Bundesländern, sowie weiteren zu beteiligenden Stellen, wie etwa der BDBOS, den Katastrophenschutzbehörden oder den kommunalen Spitzenverbänden angestrebt, da einerseits infrastrukturelle Gegebenheiten auf allen Ebenen gegenseitig hilfreich sein können und andererseits die operative Bedeutung ausgewählter Standorte bewertet werden muss.

3.1.2 Erhöhung der Verfügbarkeit im Sinne der §§ 164, 185 in Verbindung mit § 167 TKG

Die Verpflichtungen nach §§ 164, 185 TKG gelten je Betreiber bzw. Anbieter. Eine Erhöhung der Verfügbarkeit ist daher grundsätzlich netz- bzw. dienstindividuell zu betrachten, da bei netz- bzw. dienstübergreifenden Betrachtungen mit sehr hohen verfahrens- und wettbewerbsrechtlichen Hürden zu rechnen ist. Dies gilt insbesondere vor dem Hintergrund einschlägiger gesetzlicher Vorgaben, wie etwa des § 106 TKG, bei dem die Bundesnetzagentur Betreiber eines öffentlichen Mobilfunknetzes dazu verpflichten kann, in einem räumlich umgrenzten Gebiet die Mitnutzung passiver Infrastrukturen oder, soweit dies nicht ausreicht, Roaming (lokales Roaming) zu ermöglichen. Aufgrund dessen muss eine Umsetzung und Bewertung der Maßnahmen zweckmäßigerweise jeweils auf der Grundlage der konkreten Netzstrukturen und Verantwortlichkeiten der betroffenen Netzbetreiber erfolgen. Allerdings könnte auch hier ein Potenzial zur Steigerung von Effektivität und Effizienz darin liegen, die erforderliche Infrastruktur und Einrichtungen - wo immer rechtlich und technisch möglich - nicht anbieter- bzw. betreiberscharf abzugrenzen.

Es ist beabsichtigt, eine weitere Härtung der Netze zum Schutz vor Ausfällen mit technischen Mitteln vorzunehmen. Hierzu zählen insbesondere die Ausweitung bzw. Verstärkung von Strom- und Energiepuffersystemen, etwa in Form von unterbrechungsfreien Stromversorgungen (USV) sowie Netzersatzanlagen (NEA). Dabei soll angestrebt werden, bestehende Batteriepufferzeiten, soweit technisch möglich und im Rahmen der Verhältnismäßigkeit vertretbar, auf ein sinnvolles Niveau anzuheben., Die

konkrete Ausgestaltung ist pro Standort anhand der jeweiligen Netzinfrastruktur, der Störfallannahmen sowie der Kosten-Nutzen-Bewertung festzulegen. Bei gemäß der unter 3.1.1 genannten Kriterien besonders relevanter Standorte könnte – ebenfalls unter Wahrung der Verhältnismäßigkeit – auch eine längere Batteriepufferzeit geprüft werden.

Der bereits vorhandene physische Sabotageschutz der TK-Anlagen ist einer erneuten Überprüfung zu unterziehen und bei Bedarf zu erweitern. Ziel ist es, bestehende Schutzmaßnahmen hinsichtlich Wirksamkeit, Abdeckung potenzieller Angriffspfade sowie praktischer Umsetzbarkeit in Bezug auf relevante Bedrohungsszenarien zu bewerten und gegebenenfalls zusätzliche technische und organisatorische Vorkehrungen zu veranlassen, um die Anfälligkeit gegenüber vorsätzlichen Störungen nachhaltig zu reduzieren. Dabei müssen ggfs. Standorte stärker berücksichtigt werden, die in dem nach 3.1.1. gewählten Asset-Management als potenziell herausgehobene Standorte identifiziert wurden.

Die Redundanzvorgaben des Sicherheitskatalogs gemäß § 167 TKG sind zwingend einzuhalten. Darüber hinaus sollen die Netze bzw. wesentliche Netzbestandteile so redundant wie möglich ausgelegt werden, soweit dies mit den jeweiligen technischen Gegebenheiten, den Sicherheitszielen und den wirtschaftlichen Rahmenbedingungen vereinbar ist. Eine solche erhöhte Redundanz kann beispielsweise durch stark vermaschte Netzstrukturen, durch parallel betriebene Netzknoten sowie durch die Vorhaltung mehrerer Kernrechenzentren - Core Data Center (CDC's) erreicht werden, um die Fortführung des Betriebs auch bei Ausfällen einzelner Komponenten sicherzustellen.

Mobile Basisstationen (MRT) können bei Zerstörung oder erheblicher Beeinträchtigung der bestehenden Infrastruktur kurzfristig als Übergangslösung genutzt werden. Dies dient insbesondere dazu, die Kommunikationsfähigkeit in betroffenen Gebieten so schnell wie möglich wiederherzustellen und die Zeit bis zur Wiederaufnahme des Regelbetriebs durch eine temporäre, funktionsfähige Netzabdeckung zu überbrücken. Hierbei könnte es auch zielführend sein, die bereits etablierten Prozesse Provider- und Länderübergreifend weiterzuentwickeln.

Die Verbesserung der Verfügbarkeit der Telekommunikation führt unmittelbar zu einer erhöhten Verfügbarkeit des Notrufs. Damit wird nicht nur die allgemeine Kommunikationsfähigkeit gestärkt, sondern auch die Funktionssicherheit der Notrufkommunikation im Ereignisfall nachhaltig abgesichert, sodass auch in der Krise Hilfeleistungen möglichst verlässlich eingeleitet werden können.

3.1.3 Einbeziehung satellitengestützter Lösungen

Kommunikationsmöglichkeiten durch satellitengestützte Systeme könnten zusätzlich genutzt werden, um die Fähigkeiten der TK-Infrastruktur insbesondere in Ausfallszenarien oder bei eingeschränkter terrestrischer Verfügbarkeit zu erweitern und damit die Funktionssicherheit der Kommunikationsdienste insgesamt zu verbessern.

Als mittelfristig einsetzbares Szenario könnte die Nutzung von Direct-to-Device - Mobile Satellite Service (D2D-MSS) sowie Direct-to-Device - International Mobile Telecommunications (D2D-IMT) betrachtet werden, um den direkten Endgerätezugang über Satellitentechnologien als resiliente Ergänzung zu terrestrischen Netzen zu ermöglichen und damit die Kommunikationsabdeckung in Krisen- und Katastrophenlagen weiter zu erhöhen.

Derzeit verfügt bereits ein kleiner Anteil von-Smartphones über die Möglichkeit, eine Konnektivität mittels direkter Satellitenverbindungen bereitzustellen. Für die nächsten Jahre ist damit zu rechnen, dass der Anteil an diesen Smartphones, die entsprechende Funktionen unterstützen, weiter zunehmen wird und den Nutzerinnen und Nutzern zumindest eine grundlegende direkte satellitengestützte Kommunikationsmöglichkeit offerieren könnte. Vor diesem Hintergrund ist im zeitlichen Verlauf von einer Steigerung der Marktdurchdringung sowie der praktischen Einsatzfähigkeit dieser Technologie auszugehen.

In dieser Annahme ist zu erwarten, dass die Resilienz von TK-Diensten sowie insbesondere die Kommunikationsmöglichkeiten in Katastrophensituationen deutlich zunehmen könnte. Ausschlaggebend hierfür ist vor allem die größere Unabhängigkeit von terrestrischen Netzen und die damit einhergehende geringere Abhängigkeit vom diesbezüglichen Stromnetz. Gleichzeitig ist anzunehmen, dass durch die weltraumgestützte Auffangmöglichkeit mit mindestens einer rudimentären Kommunikation, der unmittelbare Bedarf an umfangreichen terrestrischen Ausbau- und Verstärkungsmaßnahmen spürbar zurückgehen könnte. Dies dürfte perspektivisch zu einer erheblichen Kostenentlastung bei den terrestrischen Netzerweiterungen sowie des Umfangs der als erforderlich anzusehenden Härtung der terrestrischen TK-Infrastruktur führen. Satellitengestützte Kommunikation kann terrestrische Netze in bestimmten Ausfallszenarien ergänzen und die Kommunikationsmöglichkeiten in Katastrophenlagen verbessern. Eine Verringerung des Bedarfs an terrestrischer Härtung oder eine erhebliche Kostenentlastung kann daraus nicht generell abgeleitet werden. Vor einer solchen Bewertung sind insbesondere Verfügbarkeit, Kapazität, Endgeräteunterstützung, Innenraumversorgung, Energieabhängigkeiten der Bodeninfrastruktur, regulatorische Einordnung, Interoperabilität, Sicherheitsanforderungen, Haftung und Übergabepunkte zu Notdiensten zu untersuchen.

Es muss allerdings berücksichtigt werden, dass die Einsatzmöglichkeiten satellitengestützter Kommunikation in bestimmten Umgebungen begrenzt sind. Insbesondere in tiefen Straßenschluchten sowie in Innenräumen ist aufgrund von Abschattungen, Gebäudeeinflüssen und ungünstigen Ausbreitungsbedingungen mit Einschränkungen der Verfügbarkeit und Verbindungsqualität zu rechnen, sodass hierfür ergänzende technische oder organisatorische Maßnahmen vorzusehen sind.

Vor dem Hintergrund der geopolitischen Entwicklungen sollte stets auch der Aspekt der Souveränität bei der Nutzung satellitengestützter Lösungen berücksichtigt werden.

3.1.4 Erhöhung der Verfügbarkeit der Kommunikationsmöglichkeiten der Behörden

Dieser Abschnitt richtet sich nicht an die MNOs, sondern bezieht sich auf Netzplanungsaktivitäten für BOS.

Langfristig ist der Aufbau und/oder die Nutzung, neben dem bereits bestehenden TETRA-Digitalfunk-BOS, eines breitbandigen terrestrischen TK-Netzes für Belange der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) vorzusehen, wobei vorrangige Zielsetzung ist, für die bedarfsgerechte und eigenständige Kommunikationsfähigkeit dieser Einheiten, insbesondere in Lage- und Einsatzszenarien mit erhöhtem Bedarf an Verfügbarkeit, Kapazität und Funktionssicherheit sicherzustellen.

Soweit möglich, sollte die Erreichbarkeit des Netzes bevorzugt so ausgestaltet werden, dass die Bevölkerung als potenzielle Kommunikationsadressaten im z.B. Katastrophenfall berücksichtigt wird (bspw. Broadcast). Hierdurch kann im Ereignisfall die Kommunikationslage verbessert werden, ohne dass die Einsatzkommunikation der BOS-Anforderungen einsatztaktisch – zu viele Nutzer in einer Zelle oder

technisch – durch die Krise ausgelöstes, deutlich erhöhtes Einbuchungsverhalten der Bevölkerung in das BOS-Netz, was mit einem distributed denial of service (DDOS)-Angriff auf das Netz vergleichbar wäre – konterkariert wird.

Die Netztopologien können sich dabei an derjenigen Bedarfstopologie orientieren, die dem Aufbau des BOS-Netzes zugrunde gelegt wird. Dies bedeutet, dass die Ausgestaltung der Topologie grundsätzlich davon abhängt, ob das Netz ausschließlich BOS-spezifische Bedarfe zu bedienen hat oder ob darüber hinaus weitere Zielgruppen bzw. zusätzliche Bedarfe mit abzudecken sind; entsprechend ist die Netzstruktur in ihrem Umfang, ihrer Verschaltung und ihrer betrieblichen Auslegung im jeweiligen Fall differenziert festzulegen.

Entsprechendes gilt für die Auswahl geeigneter Frequenzen. Auch hier ist die Frequenzplanung unmittelbar am konkreten Bedarfsprofil auszurichten, insbesondere hinsichtlich Versorgungszielen, Verfügbarkeitsanforderungen, Reichweiten- und Durchdringungseigenschaften sowie möglicher Koordinierungs- und Betriebsbedingungen, die sich je nach Umfang und Zielsetzung des jeweiligen Netzes unterscheiden können.

Bei der Konzeption, Planung und Umsetzung dieser BOS-übergeordneten Netze sind die zuvor beschriebenen Maßnahmen grundsätzlich zu berücksichtigen, insbesondere im Hinblick auf ein belastbares Assetmanagement. Dadurch soll eine konsistente Erfassung, Bewertung und Steuerung der wesentlichen Netzressourcen (insbesondere Ausleuchtung, Notstromversorgung, Funktechnologie, Frequenzen und Versorgungsparameter) gewährleistet werden, um die Umsetzung der Härtungs- und Redundanzanforderungen zielgerichtet, nachvollziehbar und effizient zu gestalten.

Die BOS-TK-Infrastruktur ist nach einem eigenen, an den konkreten BOS-Bedarf angepassten Bedarfskonzept zu härten. Dabei sind - analog zu den sicherheits- und redundanzbezogenen Anforderungen öffentlicher TK-Netze - vergleichbare technische und organisatorische Maßnahmen umzusetzen, um die Widerstandsfähigkeit gegen Ausfälle, Störungen und Schadereignisse zu erhöhen sowie die Funktionsfähigkeit auch bei außergewöhnlichen Einsatz- und Schadenslagen aufrechtzuerhalten.

Die BDBOS kann kurz- und mittelfristig Zugangsmöglichkeiten zu vorhandenen TK-Netzen anstreben, wobei sie insbesondere Zugänge zu Netzen öffentlicher Anbieter in den Blick nimmt. Dabei ist auch zu prüfen, inwieweit die gleichzeitige bzw. parallele Nutzung von Infrastruktur mehrerer Anbieter technisch, rechtlich und organisatorisch umsetzbar wäre, um eine erhöhte Resilienz zu erreichen und Abhängigkeiten von einzelnen Netzen oder einzelnen Versorgungswegen zu reduzieren.

3.2 Notruf und öffentliche Warnungen

Resilienz des Notrufs – mögliches Beteiligungsverfahren nach § 164 Absatz 6 TKG Die Technische Richtlinie Notrufverbindungen Ausgabe 2.1 (TR Notruf 2.1) wurde im Amtsblatt Nr. 13 der Bundesnetzagentur vom 9. Juli 2025 (Verfügung Nr. 66/2025) bekannt gegeben. Auf Grundlage des § 164 Absatz 6 TKG und der Verordnung über Notrufverbindungen (NotrufV) legt die Technische Richtlinie technische Einzelheiten zu Notrufverbindungen fest.

Vorbehaltlich einer etwaigen Anpassung der beiden oben genannten Rechtsgrundlagen ist die Bundesnetzagentur bestrebt, möglichst zeitnah in ein neuerliches Beteiligungsverfahren zur zeitgerechten Umsetzung der ggf. veränderten Regelsetzungsvorgaben einzutreten. Dies könnte insbesondere auch

Vorgaben zur jederzeitigen und unverzüglichen Herstellbarkeit von Notrufverbindungen und damit die von der Motivation dieses Strategiepapiers erfassten Resilienzaspekte des Notrufs betreffen.

Zur Eröffnung eines solchen Verfahrens wird die Bundesnetzagentur die gesetzlich beteiligungsberechtigten Stellen im Wege einer Amtsblattmitteilung zur Abgabe von Beiträgen und Stellungnahmen aufrufen.

Beteiligungsberechtigt nach § 164 Absatz 6 TKG sind:

- Verbände der durch § 164 Absatz 1 bis 4 TKG betroffenen Anbieter von Telekommunikationsdiensten und Betreiber von Telekommunikationsnetzen,
- vom Bundesministerium des Innern benannte Vertreter der Betreiber von Notrufabfragestellen und
- Hersteller der in den Telekommunikationsnetzen und Notrufabfragestellen eingesetzten technischen Einrichtungen.

Das Beteiligungsverfahren soll möglichst transparent gestaltet werden. Die Veröffentlichung von Beiträgen und Stellungnahmen ist daher grundsätzlich vorgesehen. Abhängig vom Umfang und Inhalt der abgegebenen Beiträge und Stellungnahmen kann die Einrichtung thematischer Arbeitsgruppen durch die Bundesnetzagentur erfolgen.

Die derzeit gültige TR Notruf 2.1 hat sich in der Anwendungspraxis bewährt. Insofern sieht die gegenwärtige Planung vor, die TR im Falle einer nur punktuellen inhaltlichen Anpassung der maßgeblichen Rechtsgrundlagen (§ 164 TKG und NotrufV) nicht vollständig neu zu erstellen. Etwaige Umsetzungs- und Anpassungserfordernisse sollen im Wesentlichen modular oder fortschreibend eingefügt werden. Dies soll die notwendige Kontinuität in diesem wichtigen Bereich der Daseinsvorsorge für alle Betroffenen und Beteiligten sicherstellen.

Insbesondere nach dem Vorliegen einer novellierten Mobilfunk-Warn-Verordnung und analog zum oben dargestellten Verfahren zur Festlegung technischer Einzelheiten zu Notrufverbindungen kommt auch die ergänzende Einleitung eines Beteiligungsverfahrens zu Resilienzaspekten der „Öffentlichen Warnung“ mittels DE-Alert nach § 164a Absatz 5 TKG in Betracht.

3.3 Organisatorische Gestaltungsoptionen des Krisenmanagements an der Nahtstelle zur Telekommunikation

Basierend auf den im Rahmen der Fortschreibung des Strategiepapiers geführten Gesprächen mit den Mobilfunknetzbetreibern (MNOs) sowie den Beratungen in verschiedenen Bund-Länder-Ausschüssen und Arbeitskreisen wurden die nachfolgenden Handlungsfelder und Gestaltungsoptionen identifiziert. Diese sollen im weiteren Verfahren durch die jeweils zuständigen Bund-Länder-Gremien fachlich konkretisiert, geprüft und hinsichtlich ihrer Umsetzbarkeit weiterentwickelt werden. Dabei sind insbesondere bestehende rechtliche, organisatorische und technische Rahmenbedingungen sowie mögliche Wechselwirkungen zwischen den einzelnen Maßnahmen zu berücksichtigen.

3.3.1 Bevölkerungs- und Katastrophenschutz bzw.Zusammenarbeit mit den MNOs

3.3.1.1 Optimierung von Meldeketten

Es sollen belastbare, institutionenübergreifende und möglichst personenunabhängige Melde- und Kommunikationsstrukturen zwischen Behörden und Mobilfunknetzbetreibern geschaffen werden. Ziel ist es, im Krisenfall einen schnellen, verlässlichen und eindeutig geregelten Informationsfluss sicherzustellen. Hierzu können beispielsweise feste Funktionspostfächer und Hotlines eingerichtet werden, sodass die Kommunikation nicht ausschließlich von einzelnen persönlichen Kontakten abhängt. Die Meldeketten sollten bereits im Vorfeld vorbereitet und regelmäßig überprüft werden.

3.3.1.2 Einheitliche Koordinierungsstelle, virtuelles Lagezentrum

Es ist zu prüfen, wie eine zentrale und ressortübergreifend vernetzte Koordinierungs- und Informationsstruktur geschaffen werden kann, über die Behörden und Mobilfunknetzbetreiber im Krisenfall ein gemeinsames Lageverständnis entwickeln und Maßnahmen abstimmen können. Eine solche Stelle könnte beispielsweise als zentrale Anlaufstelle für Meldungen und Lageinformationen dienen und durch ein virtuelles Lagezentrum ergänzt werden, in dem relevante Informationen digital gebündelt und aktuell bereitgestellt werden. Dabei sollte möglichst auf bereits vorhandenen behördlichen Systemen aufgebaut und deren Nutzung für Krisenlagen bedarfsgerecht erweitert werden.

3.3.1.3 Krisenübungen als Vorbereitung

Durch regelmäßige gemeinsame Krisenübungen sollen Strukturen, Zuständigkeiten und Abstimmungsverfahren zwischen Behörden, Mobilfunknetzbetreibern und weiteren relevanten Akteuren erprobt und gefestigt werden. Auf diese Weise können Schnittstellenprobleme oder bislang nicht berücksichtigte Handlungsbedarfe bereits vor einem tatsächlichen Ereignis erkannt werden. Ergänzend sollte geprüft werden, wie der regelmäßige Austausch zwischen Ländern, Mobilfunknetzbetreibern und Verbänden, beispielsweise über länderübergreifende Foren oder Runde Tische, dauerhaft institutionalisiert werden kann.

3.3.2 Bewegungs- und Zutrittsrechte für Einsatzpersonal

Bei der Ausgestaltung von Krisenberechtigungen sollte berücksichtigt werden, dass neben Mitarbeitern der Betreiber auch technische Dienstleister, Subunternehmer, Logistikpartner und kurzfristig eingesetzte Spezialkräfte an Wiederherstellungsmaßnahmen beteiligt sein können.

3.3.2.1 Ausgangsrechte

Es soll geprüft werden, welche rechtlichen und organisatorischen Voraussetzungen erforderlich sind, damit Krisenreaktionskräfte und notwendige Dienstleister auch bei staatlich angeordneten Ausgangs- oder Bewegungsbeschränkungen handlungsfähig bleiben. Insbesondere Entstörungs- und Reparaturkräfte der Telekommunikationsunternehmen sollten ihre Aufgaben zur Aufrechterhaltung oder Wiederherstellung der Netze weiterhin wahrnehmen können. Hierfür könnten bundesweit möglichst einheitliche und kurzfristig aktivierbare Berechtigungsnachweise vorgesehen werden.

3.3.2.2 Fahrtrechte

Die notwendige Mobilität und Transportfähigkeit von Krisenreaktionskräften, Betriebsmitteln und technischer Infrastruktur soll auch bei Fahrverboten, Sperrzonen oder sonstigen Zufahrtsbeschränkungen gewährleistet werden. Dies betrifft beispielsweise den Transport von Einsatzpersonal, Kraftstoff oder mobilen Netzersatzanlagen in betroffene Gebiete. Da sich die konkret eingesetzten Fahrzeuge im Krisenfall kurzfristig

ändern können, sollten möglichst flexible und schnell überprüfbare Berechtigungsverfahren vorgesehen werden.

3.3.2.3 Zutrittsrechte

Es sind geeignete Rahmenbedingungen zu schaffen, die einen schnellen und rechtssicheren Zugang zu kritischen Telekommunikationsstandorten für Betreiber, Dienstleister und erforderliche Spezialkräfte ermöglichen. Dies kann insbesondere dann relevant werden, wenn sich technische Anlagen innerhalb von Sperrbereichen oder auf privaten Grundstücken befinden. Ziel sollte ein möglichst länderübergreifend einheitliches Berechtigungssystem sein, das kurzfristig aktiviert werden kann und auch bei Ausfall öffentlicher Kommunikationsnetze über eine geeignete Rückfallebene verfügt.

3.3.2.4 Ersatz für elektronische Zutrittssysteme

Es ist sicherzustellen, dass der Zugang zu kritischen Telekommunikationsstandorten auch dann möglich bleibt, wenn reguläre elektronische Zutrittssysteme infolge eines Strom- oder Kommunikationsausfalls nicht mehr funktionieren. Hierfür sollten geeignete Notfall- und Rückfallverfahren vorgesehen werden, insbesondere für Standorte, die von Dritten betrieben werden. Gleichzeitig ist anzustreben, dass entsprechende Krisenberechtigungen länderübergreifend nach möglichst einheitlichen Verfahren anerkannt werden.

3.3.3 Notstromversorgung/NEAs

3.3.3.1 Emissionsrechtliche Genehmigungserleichterung im Krisenfall

Es soll geprüft werden, inwieweit emissionsrechtliche Vorgaben so angepasst oder ergänzt werden können, dass Netzersatzanlagen im Krisenfall ohne zusätzliche zeitaufwändige Genehmigungsverfahren unmittelbar eingesetzt werden können. Dies sollte insbesondere dann gelten, wenn durch den Betrieb einer Anlage die Aufrechterhaltung kritischer Telekommunikationsversorgung ermöglicht wird. Entsprechende Regelungen sollten möglichst bundesweit beziehungsweise länderübergreifend harmonisiert und auch für Mobilfunkstandorte in Schutzgebieten rechtssicher ausgestaltet werden.

3.3.3.2 Anpassung der Anzeigeverfahren im Großschadensereignis

Die bestehenden Anzeige- und Meldeverfahren sollen daraufhin überprüft werden, ob sie im Großschadensereignis einen schnellen und lagegerechten Überblick über die Auswirkungen auf Telekommunikationsnetze ermöglichen. Dabei sollte der Schwerpunkt auf wenigen für die Lagebewertung und Koordinierung relevanten Informationen liegen. Anstelle zahlreicher Einzelmeldungen, beispielsweise über jede eingesetzte mobile Netzersatzanlage, könnte eine zusammengefasste Lagebildmeldung über bestehende Krisenkommunikationsstrukturen erfolgen.

3.3.3.3 Strom-Einspeisemöglichkeiten mit standardisierten Anschlüssen an öffentlichen Gebäuden

Es ist zu prüfen, ob und an welchen kritischen öffentlichen Gebäuden standardisierte Einspeisemöglichkeiten für eine externe Stromversorgung vorgesehen werden sollten. Dadurch könnte im Krisenfall beispielsweise über eine mobile Netzersatzanlage sowohl das Gebäude selbst als auch dort installierte Mobilfunk- oder Telekommunikationstechnik versorgt werden. Eine flächendeckende Umsetzung an privaten Gebäuden oder klassischen Maststandorten erscheint dagegen nicht zwingend erforderlich und sollte nur im Einzelfall betrachtet werden.

3.3.3.4 Mitnutzung gebäudeseitiger Notstrominfrastruktur, evtl. auch von herausgehobenen Standorten

Vorhandene Notstrominfrastrukturen öffentlicher Gebäude sollen daraufhin betrachtet werden, ob sie auch zur Versorgung dort vorhandener Telekommunikationsinfrastruktur genutzt werden können. Dies könnte beispielsweise bei Verwaltungsgebäuden, Feuerwehren oder Standorten von Katastrophenschutzleuchttürmen sinnvoll sein, sofern die vorhandene Notstromversorgung ausreichend dimensioniert ist. Dadurch könnten bestehende Vorsorgestrukturen effizienter genutzt und zusätzliche parallele Notstromlösungen vermieden werden.

3.3.3.5 Krisenplan Kraftstoffversorgung

Für außergewöhnliche Krisenlagen ist zu prüfen, wie die Kraftstoffversorgung von Netzersatzanlagen auch dann gewährleistet werden kann, wenn die regulären Versorgungs- und Logistikstrukturen der Betreiber nicht mehr ausreichen. Grundsätzlich soll die Versorgung weiterhin durch die Betreiber und deren Dienstleister erfolgen; für länger andauernde oder großflächige Ereignisse sollten jedoch ergänzende staatliche Unterstützungs- und Koordinierungsmechanismen vorbereitet werden. Dazu könnten beispielsweise eine priorisierte Kraftstoffversorgung oder besondere Fahr- und Zufahrtsrechte für die notwendige Logistik gehören.

3.3.4 Bevölkerungsorientierte Optionen

3.3.4.1 Herausgehobene Standorte zur Unterstützung der Bevölkerung

Es soll geprüft werden, ob besonders resiliente und für die Bevölkerung erkennbare Standorte als feste Anlaufstellen für Krisenlagen etabliert werden können. An diesen Standorten könnte beispielsweise eine priorisierte Mobilfunkversorgung aufrechterhalten oder die Möglichkeit zum Aufladen mobiler Endgeräte geschaffen werden. Bestehende geeignete Standorte könnten hierfür gezielt gehärtet und beispielsweise durch Notstromversorgung, Festnetzanbindung oder zusätzliche Schutzmaßnahmen ergänzt werden.

3.3.4.2 Aufklärungskampagnen

Die Bevölkerung soll durch geeignete Informations- und Aufklärungsmaßnahmen besser auf mögliche Einschränkungen der Telekommunikationsversorgung vorbereitet werden. Hierzu können beispielsweise Hinweise gehören, wie Smartphones bei begrenzter Stromversorgung möglichst energiesparend genutzt werden können oder wo sich im Krisenfall der nächstgelegene besonders abgesicherte Kommunikationsstandort befindet. Ziel ist es, die Selbsthilfefähigkeit der Bevölkerung zu stärken und vorhandene Kommunikationsmöglichkeiten möglichst lange und gezielt nutzbar zu halten.

3.4 Interdependenzen der Maßnahmen bzw. der Gestaltungsoptionen unter- bzw. zueinander

Die oben abschnittsweise im Zusammenhang beschriebenen Maßnahmen und Gestaltungsoptionen können bis auf wenige Ausnahmen grundsätzlich nebeneinander betrachtet werden. Z. T. ergänzen sie sich offenkundig, z. B. die Kraftstoffversorgung und der NEA-Betrieb. Darauf soll nicht näher eingegangen werden. Komplexere Zusammenhänge, die hier betrachtet werden sollen sind aber:

- Die Planung der herausgehobenen Standorte könnte in Zusammenhang stehen mit einem zu etablierenden Asset-Management, über das die Auswahl geeigneter Standorte von Basisstationen sinnvoll erfolgen kann. In diese Planung sind neben den MNOs auch die Katastrophenschutzbehörden und die BDBOS einzubeziehen, um das Schutzniveau bzgl. der Liegenschaft, der Versorgungsanbindung und des Umfelds inklusive der Mobilfunkversorgung ganzheitlich zu gestalten

- Eine sehr kosten- und zeitintensive Härtung aller Basisstationen inklusive ausgedehntem Notstrombetrieb verbietet sich vor dem Hintergrund der Tatsache, dass voraussichtlich lange vor dem Abschluss einer solchen Maßnahme Alternativlösungen wie D2D regulär bereitstehen.

4 Ausblick

Die vorliegende Fortschreibung des Strategiepapiers stellt keinen abschließenden Zustand dar, sondern einen weiteren Schritt in einem kontinuierlichen Prozess zur Stärkung der Resilienz der TK-Netze und TK-Dienste. Die in diesem Strategiepapier dargestellten Szenarien, Interdependenzen sowie Maßnahmen und Gestaltungsoptionen spiegeln den aktuellen Kenntnisstand wider und werden mit fortschreitender Erfahrung, neuen Erkenntnissen und sich verändernden Rahmenbedingungen weiterentwickelt.

Im weiteren Verlauf sollen schnellstmöglich sukzessive weitere Szenarien identifiziert und analysiert werden, die im Rahmen dieser Fortschreibung des Strategiepapiers noch nicht oder nur am Rande berücksichtigt werden konnten. Dies soll in enger inhaltlicher Abstimmung zwischen Bund und Ländern erfolgen, da viele der betrachteten Bedrohungslagen sowohl bundesweite als auch landesspezifische Aspekte berühren und nur im koordinierten Zusammenwirken sinnvoll bearbeitet werden können.

Die Bundesnetzagentur wird den hierfür erforderlichen Dialog mit den beteiligten Unternehmen, Verbänden und Behörden auch weiterhin koordinieren und aktiv begleiten und die etablierten Strukturen für eine kontinuierliche Weiterentwicklung der Resilienzstrategie im Bereich Telekommunikation nutzen und weiter ausbauen. Die in dieser Version des Strategiepapiers festgehaltene Ergebnissicherung aus den Vorfällen in Berlin mit dem Fokus auf den Mobilfunk und das Szenario eines Stromausfalls dient als Grundlage, zukünftig auch mit weiteren zu beteiligenden Akteuren, wie beispielsweise den Breitbandnetzbetreibern und den Rechenzentrumsbetreibern in einen gemeinsamen Resilienzdialog zu kommen.

5 Anhang

Im Zuge der Erstellung der Fortschreibung V1.9 dieses Strategiepapiers wurden fachliche Diskussionen geführt mit:

- Bundesministerium für digitales und Staatsmodernisierung (BMDS)
- Bundesministerium des Inneren (BMI)
- Vertreter der Bundesländer und deren Ministerien und Arbeitsgruppen
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
- 1&1 AG
- Deutsche Telekom AG
- Telefónica Deutschland Holding AG
- Vodafone GmbH

Darüber hinaus wurden weitere Behörden und Verbände im Rahmen der Konsultation des Entwurfs einbezogen:

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS)
- Bundesverband Breitbandkommunikation (BREKO)
- Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW)
- Bundesverband Glasfaseranschluss e.V. (BUGLAS)
- ANGA der Breitbandverband
- Branchenverband der deutschen Informations- und Telekommunikationsbranche (BITKOM)
- Verband der Anbieter von Telekommunikations- und Mehrwertdiensten (VATM)
- Verband kommunaler Unternehmen e.V. (VKU)
- Verband der Internetwirtschaft (eco)

Abkürzungsverzeichnis

APT	Advanced Persistent Threat
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BMDS	Bundesministerium für Digitales und Staatsmodernisierung
BMI	Bundesministerium des Innern
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDC's	Core Data Center
D2D-IMT	Direct-to-Device - International Mobile Telecommunications
D2D-MSS	Direct-to-Device - Mobile Satellite Service
DDOS-Angriff	distributed denial of service Angriff
EKEK	Europäischer Kodex für die elektronische Kommunikation
IMS	IP Multimedia Subsystem
IXP	Internet Exchange Point
LEMP	Lightning Electromagnetic Pulse
LSA	Limited Service Access
MNOs	Mobilfunknetzbetreiber
MRT	Mobile Radio Trailer
NEA	Netzersatzanlagen
NEMP	Nuclear Electromagnetic Pulse
RCS	Rich Communication Services
SPOC	Single Point of Contact
SSOT	Single Source of Truth
TK	Telekommunikation

TKG	Telekommunikationsgesetz
USV	Unterbrechungsfreie Stromversorgung

Impressum

Herausgeber

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Tulpenfeld 4

53113 Bonn

Bezugsquelle | Ansprechpartner

Abteilung 2

Tulpenfeld 4

53113 Bonn

notfallvorsorge@bnetza.de

Stand

November 2026

Text

Abteilung 2 und Abteilung 4



bundesnetzagentur.de

x.com/BNetzA
social.bund.de/@bnetza
youtube.com/BNetzA