Bundesnetzagentur

Strategiepapier

Resilienz der Telekommunikationsnetze

Resilienz der Telekommunikationsnetze

Strategiepapier

Stand: August 2022

Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen

Abteilung 2

Tulpenfeld 4
53113 Bonn
Tel.: +49 228 14-0
Fax: +49 228 14-8872
E-Mail: info@bnetza.de

Inhaltsverzeichnis

1 Einleitung, Adressaten und Zielsetzung

In der digitalisierten Welt ist unser tägliches Leben von Informationstechnik und Telekommunikation umgeben. Mit dem Ausbau von modernen Gigabitnetzen in Festnetz und Mobilfunk sind das gesellschaftliche Leben, Wirtschaftsprozesse, das Gesundheitswesen und die öffentliche Sicherheit maßgeblich von Telekommunikationsnetzen und -diensten abhängig. Ereignisse wie etwa durch den Klimawandel verstärkte Naturkatastrophen, die Coronapandemie oder die veränderte geopolitische Lage haben in der letzten Zeit die Wichtigkeit von widerstandsfähigen Telekommunikationsnetzen und -diensten aufgezeigt.

Die zuverlässige Verfügbarkeit von Telekommunikationsnetzen ist im Alltag von essentieller Bedeutung. Diese Bedeutung steigt in Katastrophen- und Krisenfällen nochmals stark an. Es bedarf heute und in Zukunft widerstandsfähiger Telekommunikationsnetze und umfangreicher Notfall- und Sicherheitskonzepte. Die großen Telekommunikationsnetzbetreiber in Deutschland sind dank zahlreicher Vorsorgemaßnahmen und Krisenpläne bereits heute gut für den Notfall gerüstet. Dennoch besteht zwischen Netzbetreibern, Verbänden und Behörden Konsens darüber, dass die Resilienz der Telekommunikationsnetze in Bezug auf diverse Bedrohungsszenarien und die aktuelle geopolitische Lage weiter gestärkt werden sollte.

Ziel dieses Strategiepapiers ist daher die Identifizierung von Handlungsfeldern und Szenarien und darauf basierend die Entwicklung von geeigneten Maßnahmen sowie die Formulierung von Handlungsempfehlungen zur Stärkung der Resilienz von öffentlichen Telekommunikationsnetzen. Die Sicherstellung der Telekommunikation bei Vorfällen und Krisen außergewöhnlichen Ausmaßes soll im Fokus stehen. Unter Resilienz wird in diesem Zusammenhang die Widerstandsfähigkeit des Netzes gegen innere und äußere Störfaktoren verstanden und die Fähigkeit, trotz dieser Einwirkungen die Stabilität und Verfügbarkeit der Telekommunikationsnetze und -dienste zu gewährleisten.

Das Strategiepapier richtet sich, gemäß der von der Bundesregierung im Juli 2022 verabschiedeten Gigabitstrategie[1], vorrangig an Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten.

Das vorliegende Strategiepapier beschreibt außergewöhnliche Bedrohungsszenarien, etwa Kriegshandlungen oder großflächige Naturkatastrophen. Extreme Fälle von lokaler Ausdehnung, welche in den vergangenen Jahren schon vorgekommen sind und immer wieder auftreten können, sind hingegen in der Regel mit den bereits bestehenden Vorkehrungen und Maßnahmen der Telekommunikationsanbieter gut zu handhaben. Grundsätzlich ist festzustellen, dass die Telekommunikationsbranche zur Bewältigung diverser Herausforderungen gut aufgestellt ist und die Telekommunikationsnetzinfrastrukturen auch mit starken Belastungen – Stand heute – gut zurechtkommen.

[1] https://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2022/050-wissing-gigabitstrategie-der-bundesregierung-verabschiedet.html

2 Aufbau und Vorgehen

Die Bundesnetzagentur hat sich bei der Erstellung des Strategiepapiers eng mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) abgestimmt. Darüber hinaus wurden Telekommunikationsnetzbetreiber sowie Telekommunikationsverbände angehört. Diese hatten im Rahmen der Erstellung die Gelegenheit, die aus ihrer Sicht für Telekommunikationsnetze besonders relevanten Bedrohungsszenarien sowie Maßnahmen zur Steigerung der Resilienz in Telekommunikationsnetzen einzubringen. Hierzu fanden sowohl multilaterale Gespräche als auch bilaterale Abstimmungen zwischen den Behörden und allen weiteren Beteiligten statt.

Um sich dem Thema der Resilienz der Telekommunikationsnetze strukturiert zu nähern, wurde eine szenariobasierte Herangehensweise gewählt. Ziel hierbei war es, für ausgewählte, repräsentative Szenarien eine grobe Folgenabschätzung bezüglich der Auswirkungen auf die aktuellen Netze zu entwickeln. Diese sollte als Grundlage für die Ableitung von Maßnahmen zur Steigerung der Resilienz der Telekommunikationsnetze dienen. Zusammen mit Telekommunikationsnetzbetreibern, Telekommunikationsverbänden sowie dem Bundesamt für Sicherheit in der Informationstechnik wurden zum einen bereits bestehende Szenarien überprüft und einer Neubewertung unter Berücksichtigung von Erfahrungen aus den letzten Jahren unterzogen, zum anderen wurden auch weitere, bisher nicht berücksichtigte Szenarien betrachtet. Für die Evaluierung der Szenarien wurde, soweit möglich, auf die bestehende sachkundige Ausarbeitung des Umsetzungsplans kritische Infrastrukturen (UP-KRITIS) zurückgegriffen[2].

Identifizierte Maßnahmen zur Steigerung der Resilienz der Telekommunikationsnetze werden in diesem Strategiepapier in Kapitel 4 in zwei Kategorien aufgeteilt: technische Maßnahmen und organisatorische Maßnahmen.

Um eine Brücke zwischen den vorgestellten Maßnahmen und den betrachteten Bedrohungsszenarien zu schlagen, wurde jede Maßnahme mit einer Mapping Matrix (s. Anhang 6.2) auf die Szenarien abgebildet. Das Mapping stellt einen ungewichteten Mittelwert des Meinungsbildes aller Beteiligten dar und soll lediglich einen ersten Orientierungspunkt bei der Beurteilung der Maßnahmenwirksamkeit bieten.

3 Betrachtete Szenarien

Die nachfolgend aufgeführten Szenarien geben einen Überblick über identifizierte Handlungsbedarfe und stellen keine abschließende Auflistung dar.

Grundsätzlich ist die Schwere und das zu erwartende Ausmaß der Folgen eines Szenarios stark von der Dauer und der geographischen Ausdehnung abhängig. Darüber hinaus ist darauf hinzuweisen, dass die Folgen der einzelnen Szenarien meist auch andere kritische Infrastrukturen, wie beispielsweise Lebensmittelversorgung, Verkehr oder Finanzwesen betreffen, die hier jedoch mit Ausnahme der Energieversorgung nicht betrachtet werden.

[2] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/Publikationen/publikationen_node.html

3.1 Störung der Energieversorgung

Der Betrieb der Telekommunikationsinfrastruktur ist in erheblichem Maß von der Stromversorgung abhängig. Der Ausfall von Telekommunikationsinfrastruktur in Folge einer Störung der Energieversorgung kann schwere Auswirkungen hinsichtlich der Aufrechterhaltung der Wirtschaft, des Gesundheitswesens und der öffentlichen Sicherheit haben. Im Falle eines flächendeckenden Stromausfalls ist die Aufrechterhaltung der Telekommunikationsdienste je nach Dauer und Fläche des Ausfalls gefährdet. Die Telekommunikationsanlagen und Endgeräte, die durch die Teilnehmer selbst betrieben werden, fallen meistens bei einer Störung der Stromversorgung unmittelbar aus, mit Ausnahme der mobilen Endgeräte, die für eine begrenzte Zeit in Abhängigkeit des Ladezustandes weiter funktionieren. Die Versorgung der Telekommunikationsinfrastruktur mit Strom kann durch vorgehaltene Notstrominfrastrukturen für eine Übergangszeitraum aufrechterhalten werden. Allerdings wird die Versorgung von Notstromanlagen mit Kraftstoff zunehmend schwerer, je länger der Ausfall anhält. Bei der Kraftstoffversorgung konkurrieren unterschiedliche Bedarfsträger wie zum Beispiel Sicherheitskräfte, Krankenhäuser und Katastrophenhilfe mit Telekommunikationsnetzbetreibern um knappe Ressourcen.

3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen

Naturkatastrophen oder außergewöhnliche klimatische Bedingungen mit Wirkung auf die Rechenzentren und auf Technikstandorte, in denen Leit- und Steuersysteme betrieben werden, können zu einer Störung der Steuerbarkeit der Telekommunikationsnetze führen. Hieraus kann eine regional oder überregional verringerte Leistungsfähigkeit oder Verfügbarkeit der Netze, bis hin zum Ausfall, resultieren. Durch die Folgen des Klimawandels ist in den kommenden Jahren in zunehmendem Maße mit Naturkatastrophen und außergewöhnlichen klimatischen Bedingungen zu rechnen. Nach schwerwiegenden Naturkatastrophen, wie beispielsweise der Flutkatastrophe in Westdeutschland 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 Telekommunikationsdienste 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.

Auch Sonnenstürme stellen eine außergewöhnliche Gefahr für die Integrität und die Funktionsfähigkeit der Telekommunikationsnetze dar. Je nach Intensität können beispielsweise Unterseekabel über längere Zeiträume gestört werden[3].

3.3 Wirtschaftliche Schwierigkeiten, Unruhen

Aufgrund von Sanktionen gegen andere Staaten und möglicherweise daraus folgenden wirtschaftlichen Schwierigkeiten beziehungsweise Unruhen können Mangellagen in den Bereichen Gas-, Öl- oder Energieversorgung drohen. Durch die Globalisierung und die Verlagerung von Produktionen in andere

[3] https://www.heise.de/news/Internet-Apokalpyse-Sonnenstuerme-als-grosse-Gefahr-fuer-lange-Unterseekabel-6176908.html

Länder und Regionen gibt es Abhängigkeiten sowohl bei physischen Produkten als auch im Dienstleistungsbereich. Neben den drohenden Engpässen im Bereich der Hardwareversorgung ist als direkte Auswirkung auf die Telekommunikationsnetze ein durch Energiemangel bedingter Stromausfall zu nennen. Darüberhinausgehend kann auch durch Störungen oder Einschränkungen im Import oder Export der Warenfluss zumindest zeitweise unterbrochen werden, wodurch ebenfalls ein Hardwaremangel folgen kann, beispielsweise durch eine ausbleibende Lieferung von Computerchips.

3.4 Ausfall von zentralen Internet-Infrastrukturen

Durch den Ausfall von zentralen nationalen Internet-Infrastrukturen wie Internetknotenpunkte, relevanter Datencenter, Cloudservices sowie den Ausfall wichtiger Land- oder Seekabelsysteme drohen flächendeckende Störungen der Telekommunikationsnetze. Der Ausfall eines Internetknotenpunktes in Folge von durchtrennten Versorgungskabeln, beispielsweise durch Bauarbeiten oder mutwillige Beschädigung (siehe Kapitel 3.6), kann zu weitreichenden Störungen von Telekommunikationsdiensten führen. Zahlreiche Kundinnen und Kunden sind in solch einem Fall ohne Internetzugang, darunter auch Betreiber kritischer Infrastrukturen und Einrichtungen mit gesellschaftlicher Bedeutung.

Land- und Seekabelsysteme transportieren den Großteil des weltweiten Datenverkehrs. Bei einem Ausfall eines oder mehrerer Kabelsysteme wird zunächst eine Umleitung des Datenverkehrs auf andere Kabel etabliert. Im schlimmsten Fall kann daraus jedoch bei ungünstiger Positionierung der Schäden auch eine starke Beeinträchtigung bis hin zu einem Ausfall des Internets in Europa und darüber hinaus erfolgen[4]. Landkabel können insbesondere durch Bauarbeiten und Erdbewegungen, Seekabel durch die Fischerei und die Schifffahrt beschädigt werden. Alle Kabelsysteme können zudem auch gezielt durch Angriffe (siehe Kapitel 3.6) beschädigt werden.

Der Ausfall eines oder mehrerer bedeutender Datencenter oder internationaler oder nationaler Cloudservices kann dazu führen, dass Unternehmen, Universitäten und alle Personen, die den betroffenen Cloudservice nutzen, nicht mehr auf diesen zugreifen können. Aufgrund des Rückbaus von lokalen Servern und der Auslagerung der Daten in externe Datencenter und Daten-Clouds hat solch ein Ausfall massive Einschränkungen in den Geschäftsabläufen der Unternehmen und in der Effektivität Ihrer Business-Continuity-Pläne zur Folge.

3.5 Pandemien

Wie die Coronapandemie gezeigt hat, birgt eine weltweite Pandemie das Potential, die gesamte Weltwirtschaft ins Stocken zu bringen, beispielsweise aufgrund personeller Engpässe, etwa durch hohe Krankenstände, Ausgangssperren und Abriegelung ganzer Städte oder Regionen. Besonders kritisch sind in diesem Zusammenhang die Dienstleistungsbereiche sowie Technik und Logistik. Störungen in diesen Bereichen können weitreichende Auswirkungen auf sämtliche kritische Infrastrukturen haben und können Produktionsstillstände und daraus resultierende Lieferengpässe, insbesondere im Bereich der Hardware- und Kraftstoffversorgung mit sich bringen. Betrachtet man die Telekommunikationsnetze, so kann ein Versorgungsengpass bedeuten, dass notwendige Ersatzteile zur Instandhaltung der Netze nicht geliefert

[4] Vgl. Zweite Internet Backbone-Studie (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ZwiBACK/ZwiBACK-Studie.html)

werden können. Dies kann eine temporäre Reduzierung der Leistungsfähigkeit und Verfügbarkeit der Telekommunikationsnetze zur Folge haben.

3.6 Mutwillige Zerstörungen, Manipulationen, Anschläge, kriegerische Auseinandersetzungen, Sabotage und Spionage

Aufgrund der vielfältigen möglichen Szenarien und deren Auswirkungen wurden weitere Fallunterscheidungen getroffen. Es ist möglich, dass die dargestellten Szenarien kombiniert auftreten. In einem solchen Fall können sich im Bereich der schadhaften Auswirkungen Kettenreaktionen ergeben, welche das Schadenspotential vervielfachen.

3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage

Mittels mutwilliger Zerstörungen, Manipulationen oder Sabotage besteht die Möglichkeit, die Telekommunikationsinfrastruktur an einem oder mehreren Punkten in ihrer ordnungsgemäßen Funktion zu zerstören beziehungsweise zu beeinträchtigen. Als Beispiel wäre hier die Trennung oder Zerstörung von Kabeln und Knotenpunkten oder die Beschädigung oder Zerstörung von Komponenten oder Ausrüstungen von Telekommunikationsnetzen zu nennen. Da es sich um eine mutwillige Zerstörung handelt, muss bei entsprechender Verfügbarkeit von Ressourcen mit einem mehrfachen, sowohl zeitlich als auch regional abgestimmten Vorgehen, gerechnet werden. Bei Fernverbindungen bestehen beispielsweise nur eine sehr geringe Anzahl an physischen Kabelsystemen (Dark Fiber), welche von einer Vielzahl von Diensteanbietern genutzt werden, aufgrund dessen handelt es sich hierbei um Ziele, mit besonders weitreichenden Auswirkungen, für die erhöhte Georedundanzmaßnahmen (siehe Kapitel 4.1.4.) zu treffen sind. Je nach Schwere des Eingriffs können sich, bis zum Ersatz der betroffenen Hardware, nachhaltige Störungen in den Telekommunikationsnetzen und -diensten einstellen.

3.6.2 Kriegerische Auseinandersetzung, Anschläge

Durch gezielte Luft- oder Bodenangriffe auf Telekommunikationsinfrastruktur im Rahmen einer kriegerischen Auseinandersetzung wird die Infrastruktur möglicherweise nachhaltig zerstört. Ein Andauern der Kampfhandlungen in den betroffenen Gebieten oder auf den Zufahrtswegen kann zeitweilig eine Instandsetzung der betroffenen Objekte verhindern. Gegebenenfalls ist in einem solchen Szenario auch mit weiteren Einflussfaktoren wie einem flächigen Stromausfall zu rechnen. Weiterhin gilt es zu berücksichtigen, dass durch technische Entwicklungen wie beispielsweise Drohnen hochpräzise, gezielte Anschläge gegen Infrastrukturen auch für nichtstaatliche Akteure wie Terrorgruppen oder Einzelpersonen ermöglicht werden.

3.6.3 Spionage

Telekommunikationsnetze und -dienste können durch Spionage mittelbar in ihrer ordnungsgemäßen Funktion und Verfügbarkeit beeinträchtigt werden. Die Folgen von Spionage können beispielsweise mutwillige Zerstörungen und Manipulationen (Kapitel 3.6.1) umfassen. Spionage ist nicht nur durch Externe wie beispielsweise Geheimdienste anderer Staaten möglich, sondern auch durch interne Kräfte wie Mitarbeitende der Telekommunikationsunternehmen oder deren Zulieferer. Schutzmaßnahmen sollten demzufolge umfassend und in jede denkbare Richtung ausgestaltet werden.

3.6.4 Elektromagnetischer Puls (nuklear und nichtnuklear)

Ein elektromagnetischer Puls kann zum Ausfall ungeschützter elektrischer und elektromechanischer Geräte sowie zu einem Stromausfall von unbestimmter Dauer führen. Als Ursache für einen elektromagnetischen Puls kommt neben einer unnatürlichen Ursache (bspw. Sprengkörper) auch eine Naturkatastrophe (bspw.

Sonnensturm) in Betracht. Ein Wiederherstellen der Infrastrukturen nach einem elektromagnetischen Puls ist sehr aufwendig, da im schlimmsten Fall von Grund auf jegliches Gerät ersetzt werden muss. Je größer der elektromagnetische Puls, desto eher ist eine Wiederherstellung der Funktion aufgrund der Schadensausdehnung und des Umfangs mit einem Neubau jeglicher elektronischen Infrastruktur gleichzusetzen.

3.7 Über das normale Maß hinausgehende Cyberattacken

Gezielte und massive Cyberattacken auf die kritische Basisinfrastruktur können verheerende Folgen für die Wirtschaft und die öffentliche Sicherheit haben. Sie bedrohen grundsätzlich alle Unternehmen. Beispiele für diese Angriffe sind gezielte Ransomware-Attacken, welche den Zugriff auf Daten und Systeme einschränken können oder massive Distributed Denial of Service (DDoS) Angriffe gegen einzelne Dienste oder Einrichtungen. Ein weiteres mögliches, bereits aktives Szenario ist „Expect-the-breach": Dabei geht man davon aus, dass Cyberspionage vor allem staatlicher bzw. staatlich unterstützter Gruppen mit ausreichenden zeitlichen, finanziellen, personellen und fachlichen Ressourcen bereits weit vor einer kriegerischen Auseinandersetzung beginnt und das im Rahmen von Cyberspionage bereits sämtliche Netze kompromittiert wurden. Hierbei kann vor allem das Mithören oder Mitlesen des Datenverkehrs (bei verschlüsselter Kommunikation vor allem Metadaten oder Entschlüsselung) ein Hauptziel solcher Akteure sein, um Informationsgewinnung zu betreiben und gegebenenfalls spätere Sabotage vorzubereiten.

4 Ableitung möglicher Maßnahmen

Die Coronapandemie und die damit verbundenen Ausnahmesituationen haben die große Bedeutung leistungsfähiger digitaler Netze und Infrastrukturen deutlich gemacht. Digitale Technologien haben zur Aufrechterhaltung des wirtschaftlichen, politischen und gesellschaftlichen Lebens beigetragen. Die Betreiber digitaler Infrastrukturen und die Telekommunikations- und Internetwirtschaft sind auch in anderen Branchen in hohem Maße systemrelevant für die Aufrechterhaltung des Betriebes.

Die Branche und die Betreiber digitaler Infrastrukturen könnten daher durchgehend als systemrelevant eingestuft und anerkannt werden, damit Dienstleister, Sicherheitsmitarbeiter und Techniker auch bei Kontaktsperren oder -einschränkungen Zugang zu ihren Einsatzorten haben und die Funktionsfähigkeit aufrechterhalten werden kann.

Neben der Absicherung gegen zukünftige Krisen und zur Stärkung der Resilienz bedarf es zusätzlicher Maßnahmen, um im Krisenfall die Funktionstüchtigkeit und den Betrieb aufrechterhalten zu können. Vor dem Hintergrund der in Kapitel 3 dargestellten Bedrohungsszenarien hat die Bundesnetzagentur mit dem Bundesamt für Sicherheit in der Informationstechnik, den Telekommunikationsanbietern sowie den Verbänden Maßnahmen identifiziert, welche die Resilienz der Telekommunikationsnetze künftig verbessern können.

Im Ergebnis ist festzustellen, dass aus Sicht der Bundesnetzagentur, des Bundesamt für Sicherheit in der Informationstechnik und der Privatwirtschaft eine zuverlässige Energieversorgung für den Betrieb der Telekommunikationsnetze unverzichtbar ist, da ein Ausfall der Energieversorgung die größte Bedrohung für die Netze darstellt. Im Krisenfall muss die Stromversorgung sowohl für Mobilfunknetze als auch für Festnetze gewährleistet sein, um Kommunikationsdienste zu ermöglichen. In diesem Zusammenhang wird darauf hingewiesen, dass die Netzbetreiber bereits heute auf freiwilliger Basis über Notstrom- und Netzersatzanlagen verfügen. Diese sind jedoch technisch bedingt nur für eine begrenzte Zeit einsatzfähig, da beispielsweise

Akkumulatoren wieder aufgeladen und Stromerzeuger mit Kraftstoff versorgt werden müssen. Über die Sicherstellung der Energieversorgung hinaus sind jedoch weitere Maßnahmen zur Sicherstellung der Funktionsfähigkeit der Mobilfunk- sowie der Festnetzinfrastrukturen notwendig.

Die Mobilfunktechnologie ermöglicht, technisch bedingt, in Katastrophenlagen in der Regel eine breitere Versorgung der Bevölkerung mit Telekommunikationsdiensten, da die „letzte Meile", also der Weg zwischen Sendemast und Endgerät, kabellos überbrückt wird. Mobile Endgeräte sind zudem weit verbreitet und verfügen über einen integrierten Akkumulator, welcher zumindest für eine begrenzte Zeit die Kommunikation ohne externe Energieversorgung ermöglicht. Ein weiterer Vorteil von Mobilfunknetzen ist die Cell Broadcast Funktionalität, über die in Katastrophensituationen Warnungen an die Endgeräte gesendet werden können. Funktionierende Mobilfunknetze sind daher bei der Betrachtung der Resilienz der Telekommunikationsnetze von besonders hoher Bedeutung.

Festnetze stellen in großen Teilen die Basis für moderne Mobilfunknetze dar, da die Mobilfunkdaten über den größten Teil der Strecke im Transport- und Kernnetz der Netzbetreiber übertragen werden. Festnetze sind daher ein unverzichtbarer Teil von Maßnahmen zur Steigerung der Resilienz der Telekommunikationsnetze. Festnetze können in bestimmten Katastrophensituationen auch selbst einen wichtigen Beitrag zur Sicherstellung der Kommunikation leisten. So ist zum Beispiel denkbar, dass Frequenzbereiche, in denen Mobilfunknetze operieren, gestört sind und damit nicht im erforderlichen Maße zur Verfügung stehen. Für solche Fälle ist es wichtig, auf ein resilientes Festnetz zurückgreifen zu können.

4.1 Technische Maßnahmen

Die nachfolgend dargestellten technischen Maßnahmen können dazu beitragen, die Resilienz der Telekommunikationsnetze und damit die Verfügbarkeit von Telekommunikationsdiensten zu verbessern. Einige technische Maßnahmen sind eigenständig umsetzbar, andere bedingen möglicherweise die Umsetzung weiterer Maßnahmen oder lassen sich nur in Kombination mit organisatorischen Maßnahmen (Kapitel 4.2) umsetzen.

4.1.1 Notstrom für Telekommunikationsnetze und Basisdiensteangebot in Krisenfällen

Eine Störung oder ein Ausfall der Stromversorgung trifft die Funktionstüchtigkeit der Telekommunikationsnetze in der Regel sofort. Die Konsequenz ist, dass Telekommunikationsdienste nur noch eingeschränkt oder gar nicht mehr genutzt werden können. Regelmäßig ist es bei einem Stromausfall nicht mehr möglich, Notrufe abzusetzen. Auch die Cell Broadcast Technologie, welche die Bevölkerung künftig über Mobilfunknetze vor Gefahren warnen soll, funktioniert nur dann, wenn eine Mobilfunkzelle verfügbar ist, in der sich das mobile Endgerät des Nutzers einbuchen kann. Eine der wichtigsten Maßnahmen zur Steigerung der Resilienz der Telekommunikationsnetze ist es daher, für den Betrieb relevante Infrastruktur der Telekommunikationsnetze mit Netzersatzanlagen sowie Technik zur unterbrechungsfreien Stromversorgung auszustatten.

Bereits heute verfügen die Betreiber von Telekommunikationsnetzen und die Anbieter von Telekommunikationsdiensten über eine Vielzahl solcher Anlagen, darunter oft auch mobile Technik, welche sich zeitnah in Krisengebiete bringen lässt. Allerdings helfen diese von den Unternehmen freiwillig und eigenfinanzierten Notstromlösungen nur bei lokalen und regionalen Ereignissen, da ansonsten eine flächendeckende Vorhaltung derartiger Anlagen geboten sein muss und es einer entsprechenden Finanzierung bedarf. Auch ist insbesondere in den ersten Stunden eines Stromausfalls kein durchgängiges

Telekommunikationsnetz zu erwarten, denn fest installierte Notstromlösungen gibt es nur an begrenzten Technikstandorten der Netzbetreiber. Sollte es zu überregionalen, lange andauernden Stromausfällen kommen, ist mit großflächigen Störungen in den Telekommunikationsnetzen zu rechnen.

Vor diesem Hintergrund wird von der Bundesnetzagentur die Maßnahme vorgeschlagen, bundesweit einheitliche Regelungen zur Notstromversorgung von Telekommunikationsnetzen zu etablieren. Bürgerinnen und Bürger sollen in Zukunft die Möglichkeit haben, auch bei einem großflächigen Stromausfall ein bestimmtes Basisdiensteangebot nutzen zu können, beispielsweise um Notrufe absetzen zu können bzw. Warnmeldungen über Cell Broadcast empfangen zu können.

Um bei einem großflächigen Stromausfall eine Basisnetzversorgung mit Mobilfunktechnologie herstellen zu können, muss nach Einschätzung der Bundesnetzagentur nicht zwingend jede Basisstation über fest installierte Notstromtechnik verfügen. Die an der Erstellung des Strategiepapiers beteiligten Netzbetreiber haben im Rahmen dessen auch signalisiert, dass nicht jeder Technikstandort mit einer Notstromversorgung ausgerüstet werden kann, beispielsweise aus brandschutztechnischen Gründen oder weil die Statik dies nicht zulässt. Allerdings kann nach Ansicht der Bundesnetzagentur die Ausstattung eines bestimmten Teils der Basisstationen ausreichen, um die Bevölkerung mit einem Basisnetz zu versorgen.

Zudem sind aus Sicht der Bundesnetzagentur weitere technische Maßnahmen denkbar, um die Reichweite der Mobilfunknetze kurzfristig zu verbessern. Netzbetreiber könnten bei Bedarf etwa eine zeitlich auf die Katastrophensituation begrenzte Erhöhung der Sendeleistung anzeigen. So kann durch eine gesteigerte Sendeleistung die Sendereichweite erhöht werden. Allerdings ist hier zu beachten, dass typischerweise nicht die Sendeleistung der Basisstationen, sondern die der Endgeräte den limitierenden Faktor darstellt. Eine derartige Maßnahme muss nach Experteneinschätzung allerdings mit besonderer Vorsicht aufgegriffen werden, da durch eine Erhöhung der Sendeleistung andere bestehende Kommunikationswege nicht gestört werden dürfen.

Eine weitere Maßnahme könnte eine Beschränkung des Mobilfunknetzbetriebs auf sogenanntes Low-Band-Spektrum (700 bis 900 MHz) sein, welches physikalisch bedingt eine höhere Reichweite besitzt. Hiermit kann der Energieverbrauch der Netze reduziert werden. Solange nur eine eingeschränkte (Notstrom-) Versorgung zur Verfügung steht, kann mit solch einer Maßnahme die Aufrechterhaltung der Mobilfunkversorgung zeitlich verlängert werden.

Infolge der begrenzten technischen Leistungsfähigkeit und Kapazität eines Basismobilfunknetzes für den Katastrophenfall ergibt sich jedoch ein im Vergleich zu gewöhnlichen Mobilfunknetzen stark eingeschränktes Diensteangebot. Datenintensive Anwendungen, welche eine hohe Kapazität und Leistungsfähigkeit im Telekommunikationsnetz erfordern, sind in diesem Fall möglicherweise nicht oder nur sehr eingeschränkt nutzbar.

3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Abbildung 1 Auszug aus der Mapping Matrix für die Maßnahme Notstrom für Telekommunikationsnetze und Basisdiensteangebot in Krisenfällen, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und

nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.1.2 Betrachtung erneuerbarer Energien zur Krisenvorsorge

Die Technische Infrastruktur der Telekommunikationsnetze ist von einer zuverlässigen Stromversorgung abhängig. Zur Überbrückung von Stromausfällen kommen heutzutage in der Regel Netzersatzanlagen zum Einsatz, die auf Batteriebasis oder mit fossilen Kraftstoffen betrieben werden. Um die Abhängigkeit von einer regelmäßigen Kraftstoffversorgung im Krisenfall zu minimieren, soll nach Meinung von Netzbetreibern, Verbänden und Behörden in Zukunft verstärkt der Einsatz von erneuerbaren Energien für Technikstandorte in Betracht gezogen werden.

Mobilfunkstandorte könnten zukünftig beispielsweise mit Batteriesystemen in Verbindung mit Photovoltaikmodulen oder mit Brennstoffzellen ausgerüstet werden, um im Notfall eine begrenzte Versorgung mit Energie zu gewährleisten. Im gleichen Schritt müsste der Stromverbrauch der Technik am Standort im Krisenfall jedoch auch deutlich reduziert werden, um eine zuverlässige Funktionalität zu gewährleisten. Dies wäre zum Beispiel durch die Reduzierung von Kapazitäten und eine damit verbundene Fokussierung auf ein begrenztes Diensteangebot realisierbar.

Betreiber von Funkturmstandorten haben bereits signalisiert, in Zukunft an immer mehr Standorten regenerative Energiequellen nutzen zu wollen, fordern in diesem Zusammenhang jedoch, die regulatorischen Rahmenbedingungen zu verbessern.

3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Abbildung 2 Auszug aus der Mapping Matrix für die Maßnahme Betrachtung erneuerbarer Energien zur Krisenvorsorge, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.1.3 Prüfung alternativer Standort-Anbindungen

An moderne Mobilfunknetze werden hohe Anforderungen in Bezug auf Datenraten, Kapazität und Latenzzeiten gestellt. Auch Zuverlässigkeit und Ausfallsicherheit sind wichtige Faktoren. Eine leistungsfähige Anbindung der Senderstandorte in Mobilfunknetzen an das Kernnetzwerk des jeweiligen Anbieters wird daher heutzutage im Regelfall entweder über eine Glasfaser-Kabelverbindung oder über eine Richtfunkstrecke realisiert, da diese Technologien die Anforderungen am besten erfüllen können.

Auch in Katastrophenfällen sind die Anforderungen an die Leistungsfähigkeit der Mobilfunknetze sehr hoch. Insbesondere wenn die üblicherweise verwendete Anbindung des jeweiligen Mobilfunkstandortes nicht mehr die gewohnte Kapazität aufweist oder gar vollständig ausgefallen ist, kann ein Fokus auf Basisfunktionalitäten wie Cell Broadcast, Notruf, Telefonie und möglicherweise auch limitierte Internetdienste gelegt werden. Diese Fokussierung ermöglicht es dem Mobilfunknetzbetreiber, in Katastrophenfällen auch andere Standortanbindungen als Glasfaserkabel und Richtfunk in Betracht zu ziehen.

Eine Möglichkeit, die bereits in Katastrophenfällen angewandt wird, kann die Anbindung einzelner Standorte mittels Richtfunkanbindung darstellen, falls die reguläre Anbindung nicht mehr zur Verfügung steht. Die Bundesnetzagentur hat solch kurzfristige provisorische Richtfunkanbindungen während der Flutkatastrophe im Westen Deutschlands 2021 bereits unbürokratisch ermöglicht. Auch eine Anbindung von Standorten via Satellit kann im Einzelfall eine adäquate Lösung sein, um ein Basisdiensteangebot für Mobilfunkteilnehmer in Katastrophengebieten darzustellen.

Die Prüfung alternativer Standortanbindungen bietet sich vorrangig für Mobilfunknetze an, da via Mobilfunk zeitgleich eine große Anzahl an Nutzern versorgt werden kann und die Endgeräte der Nutzer aufgrund von integrierten und externen Akkus auch im Falle eines Stromausfalls zumindest noch für eine begrenzte Zeit die Möglichkeit zur Kommunikation bieten.

Im Festnetz sind die Endgeräte der Nutzer heutzutage in der Regel von einer ständigen Stromversorgung abhängig. Auch die kundennahen Technikstandorte der Festnetzbetreiber sind oftmals mit aktiver Technik ausgestattet, daher ist bei einem Stromausfall auch keine Kommunikation über das Festnetz möglich. Dennoch kann es in bestimmten Katastrophenfällen sinnvoll sein, auch im Festnetzbereich alternative Standortanbindungen, etwa via Richtfunk, zu prüfen.

Abbildung 3 Auszug aus der Mapping Matrix für die Maßnahme Prüfung alternativer Standort-Anbindungen, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.1.4 Verbesserte Georedundanz

Schon heute ist das Prinzip der Georedundanz - der geographischen Trennung von technischer Infrastruktur - ein vielfach genutztes Instrument zur Steigerung der Resilienz der Telekommunikationsnetze. So kann beispielsweise Datenverkehr in der Regel problemlos auf eine andere Verbindung umgelenkt werden, wenn eine bestimmte Infrastruktur kurzfristig nicht mehr zur Verfügung steht. Auch für Ausfälle zentraler Technikstandorte halten die Netzbetreiber in Deutschland oftmals bereits georedundante Backup-Lösungen vor, um mögliche Beeinträchtigungen der Dienste zu minimieren[5].

Vor dem Hintergrund der in Kapitel 3 dargestellten Bedrohungsszenarien und der damit einhergehenden Auswirkungen auf die Netzinfrastruktur ist eine Ausweitung der Georedundanz empfehlenswert. Für wichtige Verbindungen zwischen Knotenpunkten, sowohl auf nationaler als auch auf internationaler Ebene, sollte die

[5] Vgl. Zweite Internet Backbone-Studie (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ZwiBACK/ZwiBACK-Studie.html)

Georedundanz gestärkt werden, um die Resilienz der Telekommunikationsnetze in Bezug auf die jeweiligen Bedrohungen weiter zu verbessern.

Maßnahmen zur Stärkung der Georedundanz sollten jedoch nicht nur Verbindungen zwischen Netzknotenpunkten und Netzen im Blick haben, sondern auch Verbindungen zum Endkunden.

Abbildung 4 Auszug aus der Mapping Matrix für die Maßnahme Verbesserte Georedundanz, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.1.5 Objektschutz verstärken (physische Resilienz)

Die in Kapitel 3 dieses Strategiepapiers dargestellten Szenarien stellen teilweise eine Bedrohung für die physischen Anlagen der Telekommunikationsnetze dar. So ist beispielsweise der Klimawandel mit den einhergehenden verstärkten Naturkatastrophen eine Gefahr für zahlreiche Standorte, wie etwa die Flutkatastrophe im Westen Deutschlands im Juli 2021 gezeigt hat.

Um die Resilienz der Telekommunikationsnetze zu stärken, ist künftig ein noch effektiverer Schutz der Anlagen (wie z.B. Funkmasten und Technikstandorte) gegen diese Bedrohungen notwendig. Entsprechende Maßnahmen sollten direkt bei der Planung der Anlagen und deren Standorte mitberücksichtigt werden. Beispielhaft für solche Objektschutzmaßnahmen ist etwa ein erweiterter Schutz gegen Elementarschäden bereits bei der Planung und Errichtung solcher Anlagen, möglichst auf Basis von Informationen und Berechnungen, welche die aktuellen Bedrohungen durch verstärkte Naturkatastrophen durch den Klimawandel bereits berücksichtigen.

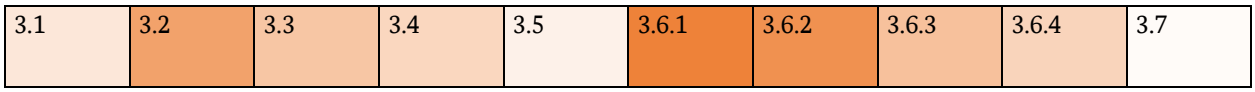

Abbildung 5 Auszug aus der Mapping Matrix für die Maßnahme Objektschutz verstärken (physische Resilienz), v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.1.6 Erweiterung von Systemen zur Angriffserkennung und -abwehr

Telekommunikationsnetze stellen nicht nur die entscheidende Schnittstelle für Cyber-Angriffe dar, sie sind auch selbst ein Ziel mit besonders weitreichenden Auswirkungen für eine große Zahl potentieller Angreifer. Die Chancen, solche Angriffe (auf die Netze und auf Teilnehmer) zu mitigieren, können durch eine frühzeitige

und effektive Angriffserkennung beträchtlich gesteigert werden. Bereits heute setzen Netzbetreiber und Diensteanbieter Systeme zur Angriffserkennung ein.

Gemäß § 8a, Absatz 1a des BSI-Gesetzes (BSIG) sind Betreiber Kritischer Infrastrukturen ab 1. Mai 2023 sogar verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dies umfasst auch den Einsatz von Systemen zur Angriffserkennung. Diese Systeme sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Entsprechend sollten diese Systeme bei der Planung der Ressourcenverteilung berücksichtigt werden.

Über die Erkennung von Angriffen hinaus hat der Gesetzgeber im § 7c BSIG in Verbindung mit § 169 des Telekommunikationsgesetzes (TKG) die Möglichkeit geschaffen, diese zur Abwehr erheblicher Gefahren auch durch technische Maßnahmen zu unterbinden. Unter anderem umfassen diese Maßnahmen die Einschränkung, Umleitung oder Unterbindung des Datenverkehrs von und zu den entsprechenden Störquellen. Auch hierzu sind durch die Anbieter von Telekommunikationsdiensten entsprechende technische und organisatorische Ressourcen bereit zu stellen.

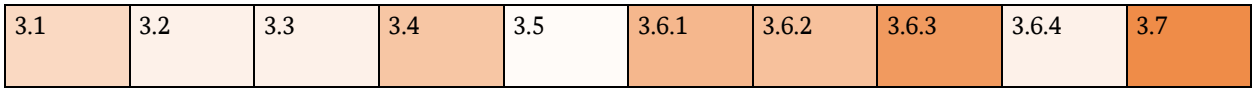

Abbildung 6 Auszug aus der Mapping Matrix für die Maßnahme Erweiterung von Systemen zur Angriffserkennung und -abwehr, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.1.7 Ausweitung von Backup-Lösungen

Backups sind eine zentrale technische Maßnahme, um die Resilienz der Telekommunikationsnetze sicherzustellen. Die Betreiber von Telekommunikationsnetzen und die Anbieter von Telekommunikationsdiensten verfügen bereits über umfangreiche und erprobte Backup- und Restorestrategien, welche im Ernstfall aktiviert werden.

Im Zuge der in diesem Strategiepapier dargestellten Bedrohungsszenarien, insbesondere in Bezug auf mögliche Cyberangriffe beträchtlichen Ausmaßes, sind möglicherweise Ausweitungen der Backup-Maßnahmen erforderlich. Institutionen sowie Industrie fordern sowohl Maßnahmen gegen den physischen als auch gegen den logischen Verlust eines Backups[6].

[6] NIST Special Publication 800-209 Security Guidelines for Storage Infrastructure: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf

Physikalischer Verlust des Backups (Beispiele):

- Diebstahl, Einbruch, Vandalismus
- Feuer, Wasserschäden
- Rauch und Gas, Staub und Schmutz
- Extreme Temperaturen
- Elementarschäden durch Erdbeben, Flut, Lawinen

Logischer Verlust des Backups (Beispiele):

- Das Backup wurde gelöscht, z.B. durch Angreifende
- Backup ist kompromittiert z.B. durch Infektion von Malware, Ransomware oder sonstige Schadsoftware die z.B. eine Backdoor enthält
- Menschliches Versagen oder absichtliche Fehlkonfiguration

Maßnahmen gegen den physikalischen Verlust des Backups (Beispiele):
Umsetzung der 3-2-1 Backup Strategie

- 3 Backups
- 2 unterschiedliche Speichermedien (insbesondere auch Nutzung von Read-only-Speichermedien, welche von Angreifenden nicht überschrieben werden können)
- 1 Kopie an einem externen Standort

Maßnahmen gegen den logischen Verlust des Backups (Beispiele):

- Vollständige organisatorische und personelle Trennung von System Administrator und Storage Administrator (Least Privilege Model und Separation of Duty)
- Backup Mitarbeiter müssen sicherheits- oder sabotageschutzüberprüft sein (SÜG)
- Backup-Systeme sollen gemäß ihrer Risikobewertung eingestuft werden und in besonderem Maße gehärtetund geschützt sein. Insbesondere ist eine Multifaktorauthentifizierung (MFA) einzuführen
- Das Backup-System muss von einem Security Information and Event Mangement (SIEM) und einem Endpoint Protection Systemüberwacht werden
- Online-Backups müssen regelmäßig durch einen Schwachstellenscanner oder eine Sandbox auf Schadsoftware überprüft werden
- Es müssen regelmäßig dokumentierte Wiederherstellungstests durchgeführt werden

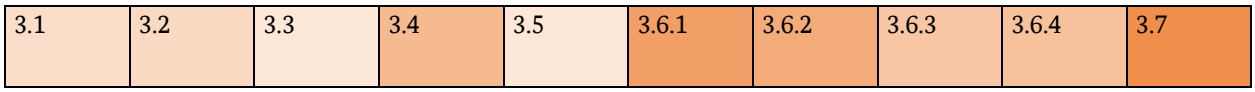

Abbildung 7 Auszug aus der Mapping Matrix für die Maßnahme Ausweitung von Backup-Lösungen, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.2 Organisatorische Maßnahmen

Neben einer Reihe von technischen Maßnahmen wurden durch die am Strategiepapier beteiligten Telekommunikationsnetzbetreiber, Verbände und Behörden ergänzend auch organisatorische Maßnahmen identifiziert, welche die Resilienz der Telekommunikationsnetze direkt oder indirekt verbessern können.

4.2.1 Gemeinsames Lagezentrum von Netzbetreibern und Behörden

Telekommunikationsnetzbetreiber, Verbände, das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur schlagen vor, ein gemeinsames Lage- und Reaktionszentrum von Telekommunikationsnetzbetreibern und zuständigen Behörden einzurichten, um in akuten Bedrohungslagen die Zusammenarbeit zwischen den verschiedenen Akteuren zu verbessern und die Koordination von Maßnahmen zu erleichtern[7].

Ein Teil des Lagezentrums sollte für die Beurteilung der aktuellen Lage der Telekommunikationsnetze rund um die Uhr mit Mitarbeitenden der relevanten Netzbetreiber und Behörden besetzt sein. Das Telekommunikationslagezentrum soll durch Informationen aller Netzbetreiber und Behörden und Organisationen (wie z.B. Technisches Hilfswerk oder auch Wetterdienste) auf kommunaler, landes- und bundesweiter Ebene gespeist werden. Hiermit soll erreicht werden, dass eine umfassende Einschätzung der aktuellen Lage erfolgen kann, um so die gebotenen Maßnahmen zur Bekämpfung einer bestimmten Katastrophensituation frühzeitig und effizient ergreifen zu können.

Das Lagezentrum soll sowohl auf virtueller als auch auf Präsenzbasis etabliert werden und durch regelmäßige Übungen (vgl. Kapitel 4.2.2) auf Krisensituationen vorbereitet werden.

Es sollten die Voraussetzungen dafür geschaffen werden, dass die am gemeinsamen Lagezentrum beteiligten Vertreter von Unternehmen und Behörden mit vertraulichen Informationen der jeweils anderen arbeiten können, beispielsweise durch entsprechende Verträge und Sicherheitsüberprüfungen. Der Schutz der individuellen Betriebs- und Geschäftsgeheimnisse muss jederzeit gewährleistet sein.

Leitung und Koordination eines solchen Lagezentrums sollte durch eine unabhängige Instanz mit klar definierten Zuständigkeiten sowie Befugnissen übernommen werden. Hierfür könnte eine bereits bestehende Behörde des Bundes vorgesehen werden.

3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Abbildung 8 Auszug aus der Mapping Matrix für die Maßnahme Gemeinsames Lagezentrum von Netzbetreibern und Behörden, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und

[7] Das gleiche Ziel verfolgt auch die Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat unter Punkt 5. „Cyber-Resilienz Kritischer Infrastrukturen stärken“ als Maßnahme für die 20. Legislaturperiode. Hier ist insbesondere eine dichte Anbindung von KRITIS-Betreibern an das BSI-Lagezentrum vorgesehen. Für jeden KRITIS-Sektor soll hierzu ein sektorspezifisches Cyber Emergency Response Team (CERT) von den KRITIS-Betreibern etabliert werden (s.: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.html)

nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.2.2 Optimierung der Zusammenarbeit durch Übungen

Die an diesem Strategiepapier beteiligten Unternehmen, Verbände und Behörden befürworten regelmäßige Übungen zur Sicherstellung der Telekommunikation in Krisenfällen. Die Übungen sollen die in Kapitel 3 dargestellten Szenarien umfassen und für die Optimierung der Zusammenarbeit zwischen Telekommunikationsnetzbetreibern, Behörden und weiteren Beteiligten sorgen.

Im Rahmen der landes- und ressortübergreifenden Krisenmanagementübung (LüKEx) ist ein derartiges Übungskonzept bereits etabliert und in den letzten Jahren mehrfach mit Erfolg durchgeführt worden.

Es erscheint jedoch sinnvoll, dass in solche oder vergleichbare Übungen in Zukunft neben den staatlichen Akteuren auch Unternehmen der kritischen Infrastruktur (KRITIS) eingebunden werden. Aus Sicht der Bundesnetzagentur sind bundesweite aber auch regionale Telekommunikationsnetzbetreiber in derartige Übungen einzubeziehen. So verfügen zum Beispiel viele kleinere Telekommunikationsnetzbetreiber über regional sehr wichtige Glasfaser-Infrastrukturen, welche im Krisenfall ebenso wichtig und erhaltenswert sind wie die Strukturen großer, überregionaler Anbieter. Weiterhin sollten die Anbieter und Betreiber von 5G-Campusnetzen in Zukunft in Abhängigkeit der jeweiligen Szenarien ebenfalls an Übungen beteiligt werden. Bei den 5G-Campusnetzen handelt es sich vielfach um Netze industrieller Produktionsstätten mit hoher wirtschaftlicher Bedeutung für die Industrie. Darüber hinaus wird angeregt, in die Übungen andere Sektoren und kritische Infrastrukturen einzubeziehen, um das Zusammenspiel im Krisenfall zu optimieren.

In Zusammenhang mit den genannten Übungen sollten verstärkt auch Stresstests zur Überprüfung der Telekommunikationsnetze auf mögliche Schwachstellen durchgeführt werden.

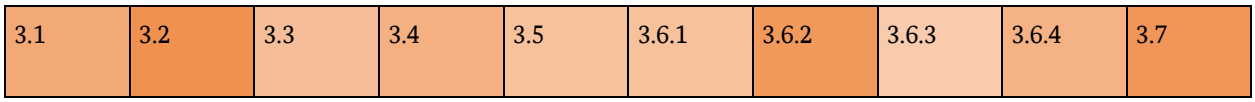

Abbildung 9 Auszug aus der Mapping Matrix für die Maßnahme Optimierung der Zusammenarbeit durch Übungen, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.2.3 Sicherstellung der Kommunikation zwischen den Akteuren in der Krise

Ein wesentlicher Faktor während Krisensituationen ist neben der internen auch eine möglichst effiziente Steuerung der externen Kommunikation (z.B. mit Behörden, Medien), welche durch eine etablierte Leitung des Lagezentrums (vgl. Kapitel 4.2.1) umgesetzt werden kann.

Darüber hinaus sind auch individuelle Maßnahmen in den jeweiligen Organisationen zu treffen, um die Kommunikation sicherzustellen. Ansprechpartner und Zuständigkeiten müssen benannt und bekannt sein sowie die Kommunikationswege für den Krisenfall regelmäßig überprüft werden.

Zwischen 2016 und 2017 untersuchte der Themenarbeitskreis Krisenkommunikationssystem unterschiedliche Kommunikationssysteme, die auch bei massiven Energie- und Informationstechnik bzw. Telekommunikationsausfällen noch verfügbar sein sollen. Ziel war es, für die Unternehmen der kritischen Infrastruktur und die zuständigen Behörden ein abgegrenztes, gemeinsames System zur Früherkennung von Informationstechnikkrisen sowie ein gemeinsames Krisenmanagementsystem mit entsprechenden hochverfügbaren (Kommunikations-)Strukturen und Prozessen zu etablieren.

In der Sitzung des Plenums des Umsetzungsplans Kritische Infrastrukturen (UP KRITIS) 01/2017 wurde der Beschluss gefasst, das Bundesministerium des Inneren und für Heimat um eine Grundsatzentscheidung unter Einbindung von Bundesamts für Sicherheit in der Informationstechnik und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe zur Nutzung, Erweiterung und Anpassung des modularen Warnsystems (MoWaS) zu bitten. Nach den Ereignissen im 1. Halbjahr 2022 (insb. KA-SAT-Ausfall) sollen mögliche technische Lösungen erneut geprüft werden. Nach Ansicht der Bundesnetzagentur kann diese Untersuchung erneut geprüft und ein Einsatz vorgeschlagen werden.

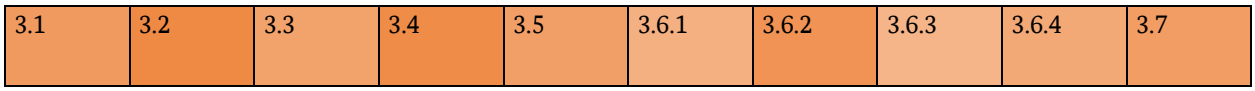

Abbildung 10 Auszug aus der Mapping Matrix für die Maßnahme Sicherstellung der Kommunikation zwischen den Akteuren in der Krise, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.2.4 Priorisierung der Energieversorgung im Knappheitsfall

Die seitens der Branche geforderte Priorisierung der Energieversorgung während einer Strommangellage und die Absicherung der Telekommunikationsnetze als kritische Infrastruktur erfordert klare politische Vorgaben. Die Versorgung von mobilen und stationären Netzersatzanlagen mit Treibstoff ist im Krisenfall eine gemeinsame Aufgabe von Unternehmen und Behörden, da die Unternehmen selbst möglicherweise keinen regulären Zugriff auf diese Ressource bekommen oder der Transport zur Verwendungsstelle nicht möglich ist.

Gleichzeitig müssen im Sinne einer umfassend verstandenen Resilienz der Telekommunikationsnetze die notwendigen Maßnahmen auf Endkundenebene betrachtet werden. Genauso wie Nahrung und Wasser stets für einige Tage bevorratet werden sollten, empfiehlt sich für Privathaushalte zur Sicherstellung der Kommunikation im Katastrophen- und Krisenfall auch eine mobile Stromversorgung (bspw. Powerbank), um Akkus von mobilen Endgeräten auch ohne externe Stromversorgung wieder aufladen zu können.

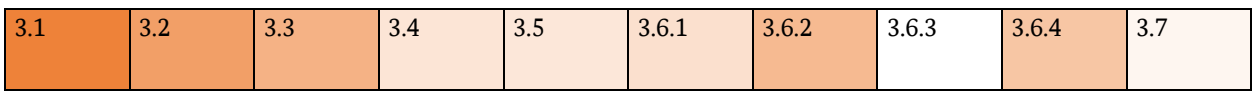

Abbildung 11 Auszug aus der Mapping Matrix für die Maßnahme Priorisierung der Energieversorgung im Knappheitsfall, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear),

3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.2.5 Schwachstellenanalyse im Bereich Netzzusammenschaltung und Netzzugang

Durch die Verbindung mit anderen Netzen ergeben sich zusätzliche Schwachstellen für Telekommunikationsnetzbetreiber, welche die Funktionsfähigkeit eines Netzes und damit die Kommunikation beeinträchtigen oder verhindern können. Folgende Maßnahmen können dieses Risiko reduzieren:

- Bereits bei der Definition von Schnittstellen sollten Sicherheitsaspekte berücksichtigt werden. Veraltete, unsichere Protokolle sollten schnellstmöglich durch sichere Produkte ersetzt werden. Wenn das nicht möglich ist, sollte der Funktionsumfang der veralteten Protokolle eingeschränkt und eine verstärkte Überwachung der Netzzusammenschaltung durchgeführt werden.
- Damit der Zutritt zu Kollokationsräumen sicher gestaltet werden kann, sind bereits heute klare und verbindliche Regelungen für die Erteilung der Zutrittserlaubnis festgelegt. Eine Mindestforderung ist, dass die Zutrittsrechte an eine einzelne Person gebunden sind. Die erteilten Zutrittsrechte sind regelmäßig zu prüfen und bei Bedarf zu entziehen. Zudem sind die Regelungen zur Erteilung der Zutrittsrechte regelmäßig auf Wirksamkeit zu prüfen und es müssen Ansprechpartner für Störungen und Sicherheitsvorfälle festgelegt werden.
- Die physische Sicherheit entspricht der des gesamten Telekommunikationsnetzes und schon bei der Planung sollten Methoden entwickelt werden, die Netztopologie nach außen zu verbergen.
- Die informationstechnischen Protokolle sollten zwischen den Partnern so abgesichert werden, dass die Integrität der Verbindung nicht gebrochen werden kann. Zudem sollte eine physikalische Trennung zwischen Steuerung und Nutzdaten vorhanden sein.

Als Maßnahmen zur Verstärkung der Resilienz bei Netzzusammenschaltungen wird Folgendes vorgeschlagen:

- Einbindung in die Notstromversorgung, um die Dienstgüte zu erhalten
- Redundante Anbindung, um die Ausfallwahrscheinlichkeit entsprechend der Priorität der Verbindung aufrecht zu erhalten
- Überwachung des Verkehrs auf Anomalien und Protokollierung von Änderungen
- Integration in das Angriffserkennungssystem

Abbildung 12 Auszug aus der Mapping Matrix für die Maßnahme Schwachstellenanalyse im Bereich Netzzusammenschaltung und Netzzugang, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

4.2.6 Schulung von Mitarbeitenden, Best Practices

Bei der Betrachtung möglicher organisatorischer Maßnahmen zur Stärkung der Resilienz der Telekommunikationsnetze sollte regelmäßig der Schulungsbedarf der Mitarbeitenden geprüft werden. Hier sollte geprüft werden, ob und inwiefern darüber hinaus die Möglichkeit besteht, die Schulungs- und Fortbildungsangebote für die Beschäftigten zu erweitern.

In besonders kritischen Bereichen ist aktuell bereits eine Sicherheitsüberprüfung der in diesen Bereichen tätigen Mitarbeitenden gefordert. Die Sicherheitsanforderungen sollten kontinuierlich auf den Prüfstand gestellt und nach Bedarf angepasst werden. Insbesondere in den nicht als kritisch eingestuften Bereichen ist eine Verschärfung der Sicherheitsanforderungen, bspw. die Zugangsregelungen zu den Gebäuden, zu empfehlen.

Darüber hinaus sind die Sensibilisierung der Mitarbeitenden und regelmäßige Informationen über potentielle Gefahren und Sicherheitslücken maßgeblich, um ein höheres Maß an Sicherheit gewährleisten zu können. Regelmäßige Kontrollen und Übungen sind ein effektives Mittel, den Wissensstand der Beschäftigten beurteilen zu können, Schulungsbedarf frühzeitig zu erkennen und notwendige Nachschulungen zu organisieren.

3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Abbildung 13 Auszug aus der Mapping Matrix für die Maßnahme Schulung von Mitarbeitern, Best Practices, v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

5 Zusammenfassung und Ausblick

Die Bundesnetzagentur empfiehlt, die digitale Infrastruktur in Deutschland resilient und nachhaltig auszubauen. Das vorliegende Strategiepapier zeigt Handlungsfelder und konkrete Maßnahmen auf, um die Resilienz der Telekommunikationsnetze und -dienste zu steigern. Diese wurden gemeinsam mit der Branche erarbeitet. Es besteht Einvernehmen in der Branche und den Behörden, an der Umsetzung von Maßnahmen mitzuwirken.

Mit Blick auf die dargestellten Maßnahmen sollte in einem ersten Schritt eine Festlegung erfolgen, welche dieser Maßnahmen prioritär auf die Umsetzungsmöglichkeiten in den Blick genommen werden. Bei der Klärung der Umsetzbarkeit von Maßnahmen sind eine Vielzahl von Folgefragen zu klären. So müssen geforderte und festgelegte technische und organisatorische Maßnahmen im Rahmen der Verhältnismäßigkeit entsprechend den Bedürfnissen und der Größe der jeweiligen Unternehmen angepasst sein; nicht jedes Unternehmen wird jede Maßnahme gleichermaßen schnell und umfassend umsetzen können, andere Unternehmen haben einige der Maßnahmen möglicherweise bereits umgesetzt.

Im Rahmen weiterer Schritte sollte festgelegt werden, welche der dargestellten technischen Maßnahmen in den Netzen umgesetzt werden sollen. Dies gilt auch mit Blick auf die zeitliche Realisierbarkeit und der

Kostentragung. Entsprechendes gilt für die dargestellten organisatorischen Maßnahmen, für die insbesondere die Verantwortlichkeiten und Handlungsabläufe festzulegen sind. Letztlich müssen gegeben falls auch rechtliche Grundlagen geschaffen werden.

Ein wichtiger Aspekt ist neben der Verwirklichung der individuell bestmöglichen Resilienz für das jeweilige Telekommunikationsnetz bzw. den jeweiligen Telekommunikationsdienst, auch eine netzübergreifende Strategie zu entwickeln und zu verfolgen. Wie dargestellt, ist es in Krisen- und Katastrophenfällen notwendig, die Gesamtheit der betroffenen Telekommunikationsinfrastrukturen (Mobilfunk und Festnetz) in den Blick zu nehmen.

Einige der in diesem Strategiepapier dargestellten Maßnahmen wie beispielsweise das gemeinsame Lagezentrum von Netzbetreibern und Behörden (vgl. Kapitel 4.2.1) erfordern zudem die aktive Zusammenarbeit von Unternehmen, Verbänden und Behörden und bedürfen weiterer Konkretisierung hinsichtlich ihrer Verantwortlichkeiten und der konkreten Ausgestaltung.

Auch finanzielle und rechtliche Aspekte müssen im Rahmen der Umsetzung von Maßnahmen geklärt werden.

Die Bundesnetzagentur regt an, in einem weiteren Schritt den Branchendialog zwischen den beteiligten Unternehmen, Verbänden und Behörden weiter fortzusetzen. Ziel ist die Umsetzbarkeit der dargestellten Maßnahmen zu eruieren und die Verantwortlichkeiten zu bestimmen. Widerstandsfähige und starke Netze erhalten die Handlungsfähigkeit aller auch und gerade in Krisenfällen und schaffen damit erst die Möglichkeit, sich den jeweiligen Herausforderungen effizient zu stellen und diese zu meistern.

6 Anhang

6.1 Beteiligte Unternehmen, Verbände und Behörden

- 1&1 AG
- ANGA der Breitbandverband
- Bundesamt für Sicherheit in der Informationstechnik
- Bundesministerium für Digitales und Verkehr
- Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
- Bundesverband Breitbandkommunikation (BREKO)
- Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW)
- Bundesverband Glasfaseranschluss e.V. (BUGLAS)
- Branchenverband der deutschen Informations- und Telekommunikationsbranche (BITKOM)
- Deutsche Telekom AG
- Telefónica Deutschland Holding AG
- Verband der Anbieter von Telekommunikations- und Mehrwertdiensten (VATM)
- Verband kommunaler Unternehmen e.V. (VKU)
- Verband der Internetwirtschaft (eco)
- Vodafone GmbH

6.2 Mapping Matrix

Die Matrix stellt die ungewichtete und gemittelte Bewertung der Beziehung von Maßnahmen und Szenario von 1&1 AG, Bundesamt für Sicherheit in der Informationstechnik, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Bundesverband der Energie- und Wasserwirtschaft e.V., Deutsche Telekom AG, OneFiber Interconnect Germany GmbH, Verband kommunaler Unternehmen e.V., Verband der Internetwirtschaft und Vodafone GmbH dar. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

Maßnahmen \ Szenarien	3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7
Technische Maßnahmen										
4.1.1 Notstrom für Telekommunikationsnetze und Basisdiensteangebot in Krisenfällen										
4.1.2 Betrachtung erneuerbarer Energien zur Krisenvorsorge										
4.1.3 Prüfung alternativer Standort-Anbindungen										
4.1.4 Verbesserte Georedundanz										
4.1.5 Objektschutz verstärken (physische Resilienz)										
4.1.6 Erweiterung von Systemen zur Angriffserkennung										
4.1.7 Ausweitung von Backup-Lösungen										
Organisatorische Maßnahmen										
4.2.1 Gemeinsames Lagezentrum von Netzbetreibern und Behörden										
4.2.2 Optimierung der Zusammenarbeit durch Übungen										
4.2.3 Sicherstellung der Kommunikation zwischen den Akteuren in der Krise										
4.2.4 Priorisierung der Energieversorgung im Knappheitsfall										
4.2.5 Schwachstellenanalyse im Bereich Netzzusammenschaltung und Netzzugang										
4.2.6 Schulung von Mitarbeitern, Best Practices										

Abbildung 14 Mapping Matrix der Szenarien und Maßnahmen, Szenarien v.l.n.r.: 3.1. Störung der Energieversorgung, 3.2 Naturkatastrophen, außergewöhnliche klimatische Bedingungen, 3.3 Wirtschaftliche Schwierigkeiten, Unruhen, 3.4 Ausfall von zentralen Internet-Infrastrukturen, 3.5 Pandemien, 3.6.1 Mutwillige Zerstörungen, Manipulationen, Sabotage, 3.6.2 Kriegerische Auseinandersetzung, Anschläge, 3.6.3 Spionage, 3.6.4 Elektromagnetischer Puls (nuklear und nicht nuklear), 3.7 Über das normale Maß hinausgehende Cyberattacken. Je dunkler die Färbung desto stärker wurde ein Zusammenhang der Maßnahme mit dem jeweiligen Szenario bewertet.

Abbildungsverzeichnis

Impressum

Herausgeber

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Tulpenfeld 4

53113 Bonn

Bezugsquelle | Ansprechpartner

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Pressestelle

Tulpenfeld 4

53113 Bonn

pressestelle@bnetza.de

www.bundesnetzagentur.de

Stand

August 2022

Druck

Bundesnetzagentur

Bildnachweis

Titel: AdobeStock, vectorfusionart

Text

Referat 217