Bundesnetzagentur

Strategy paper
Resilience of telecommunications networks

Resilience of telecommunications networks

Strategy paper

Status: August 2022

**Federal Network Agency for Electricity, Gas,
Telecommunications, Post and Railway**

Division 2

Tulip field 4
53113 Bonn
Tel.: +49 228 14-0
Fax: +49 228 14-8872
E-mail: info@bnetza.de

Table of contents

1 Introduction, addressees and Objective

In the digitized world, our daily lives are surrounded by information technology and telecommunications. With the roll-out of modern gigabit networks in fixed and mobile communications, social life, economic processes, healthcare and public safety are significantly dependent on telecommunications networks and services. Events such as natural disasters exacerbated by climate change, the Corona pandemic, and the changing geopolitical situation have recently highlighted the importance of resilient telecommunications networks and services.

The reliable availability of telecommunications networks is of essential importance in everyday life. This importance increases even further in the event of disasters and crises. Resilient telecommunications networks and comprehensive emergency and security concepts are needed today and in the future. Thanks to numerous precautionary measures and contingency plans, the major telecommunications network operators in Germany are already well equipped for emergencies. Nevertheless, there is consensus among network operators, associations and authorities that the resilience of telecommunications networks should be further strengthened in relation to diverse threat scenarios and the current geopolitical situation.

The aim of this strategy paper is therefore to identify fields of action and scenarios and, based on these, to develop suitable measures and formulate recommendations for action to strengthen the resilience of public telecommunications networks. The focus should be on securing telecommunications in the event of incidents and crises of exceptional proportions. In this context, resilience is understood as the network's resistance to internal and external disruptive factors and the ability to ensure the stability and availability of telecommunications networks and services despite these influences.

In line with the gigabit strategy1 adopted by the German government in July 2022, the strategy paper is aimed primarily at telecommunications network operators and telecommunications service providers.

This strategy paper describes extraordinary threat scenarios, such as acts of war or large-scale natural disasters. By contrast, extreme cases of local expansion, which have already occurred in recent years and may occur again and again, can generally be handled well with the precautions and measures already taken by telecommunications providers. In general, it can be said that the telecommunications industry is well positioned to cope with various challenges and that the telecommunications network infrastructures can also cope well with heavy loads - as things stand today.

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

2 Structure and Procedure

The Federal Network Agency consulted closely with the Federal Office for Information Security (BSI) in preparing the strategy paper. In addition, telecommunications network operators and telecommunications associations were consulted. During the preparation process, they had the opportunity to contribute the threat scenarios they considered particularly relevant for telecommunications networks, as well as measures to increase resilience in telecommunications networks. Both multilateral discussions and bilateral consultations took place between the authorities and all other parties involved.

In order to approach the topic of resilience of telecommunications networks in a structured way, a scenario-based approach was chosen. The aim here was to develop a rough impact assessment for selected, representative scenarios with regard to the effects on the current networks. This was to serve as a basis for deriving measures to increase the resilience of telecommunications networks. Together with telecommunications network operators, telecommunications associations and the Federal Office for Information Security, existing scenarios were reviewed and re-evaluated in the light of experience gained in recent years, and other scenarios that had not previously been considered were also examined. For the evaluation of the scenarios, the existing expert elaboration of the Critical Infrastructure Implementation Plan (UP-KRITIS) was used as far as possible2.

Identified measures to increase the resilience of telecommunications networks are divided into two categories in this strategy paper in Chapter 4: technical measures and organizational measures.

To build a bridge between the measures presented and the threat scenarios considered, each measure was mapped to the scenarios using a mapping matrix (see Annex 6.2). The mapping represents an unweighted average of the opinions of all stakeholders and is intended only to provide an initial point of reference in assessing measure effectiveness.

3 Considered scenarios

The scenarios listed below provide an overview of identified needs for action and do not represent an exhaustive list.

In principle, the severity and the expected extent of the consequences of a scenario are strongly dependent on its duration and geographical extent. In addition, it should be noted that the consequences of the individual scenarios usually also affect other critical infrastructures, such as food supply, transport or finance, which, however, are not considered here with the exception of energy supply.

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

3.1 Disruption of the energy supply

The operation of the telecommunications infrastructure depends to a considerable extent on the power supply. The failure of telecommunications infrastructure as a result of a power supply disruption can have severe consequences in terms of maintaining the economy, healthcare, and public safety. In the event of a widespread power outage, the maintenance of telecommunications services is at risk depending on the duration and area of the outage. The telecommunications equipment and terminals operated by the subscribers themselves usually fail immediately in the event of a power supply failure, with the exception of mobile terminals, which continue to function for a limited time depending on the state of charge. The supply of electricity to the telecommunications infrastructure can be maintained for a transitional period by means of emergency power infrastructures kept in reserve. However, supplying fuel to emergency power systems becomes increasingly difficult the longer the outage continues. When it comes to fuel supply, different demand drivers, such as security forces, hospitals and disaster relief, compete with telecommunications network operators for scarce resources.

3.2 Natural disasters, exceptional climatic conditions

Natural disasters or exceptional climatic conditions affecting data centers and technical sites where control systems are operated can lead to a disruption in the controllability of telecommunications networks. This may result in a regional or supraregional reduction in the performance or availability of the networks, or even in their failure. Due to the consequences of climate change, natural disasters and exceptional climatic conditions are to be expected to an increasing extent in the coming years. After severe natural disasters, such as the floods in western Germany in 2021, it is often not possible to use roads and access routes for the maintenance and repair of technical sites. This makes it difficult to supply physically intact sites with fuel or emergency power generators, in addition to the potentially necessary but unavailable repairs.

Major heat waves can limit the performance of data centers due to overloaded air-conditioning systems to such an extent that the telecommunications services offered cannot be provided to the necessary extent. In such a situation, this can also affect the energy suppliers and their networks as well as control systems themselves, which can additionally lead to a temporary energy shortage and regional network failure.

Solar storms also pose an exceptional risk to the integrity and functioning of telecommunications networks. Depending on their intensity, submarine cables, for example, can be disrupted for long periods of time3.

3.3 Economic difficulties, Unrest

Sanctions against other countries and possible resulting economic difficulties or unrest could lead to shortages in the gas, oil or energy supply sectors. Due to globalization and the relocation of production to other countries, the

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

countries and regions, there are dependencies both in terms of physical products and services. In addition to the threat of bottlenecks in the area of hardware supply, a direct impact on telecommunications networks is a power outage caused by a shortage of energy. Furthermore, disruptions or restrictions in imports or exports can also interrupt the flow of goods, at least temporarily, which can also result in a hardware shortage, for example due to a failure to deliver computer chips.

3.4 Failure of central Internet infrastructures

The failure of central national Internet infrastructures such as Internet hubs, relevant data centers, cloud services, and the failure of important land or submarine cable systems poses a threat of widespread disruption to telecommunications networks. The failure of an Internet node as a result of severed supply cables, for example due to construction work or wilful damage (see Section 3.6), can lead to widespread disruption of telecommunications services. Numerous customers are left without Internet access in such a case, including operators of critical infrastructures and facilities of social importance.

Land and submarine cable systems carry the majority of global data traffic. If one or more cable systems fail, data traffic is initially rerouted to other cables. In the worst case, however, this can also result in a severe impairment, up to and including a failure of the Internet in Europe and beyond, if the damage is positioned unfavorably4.
Land cables can be damaged in particular by construction work and earth movements, submarine cables by fishing and shipping. All cable systems can also be specifically damaged by attacks (see chapter 3.6).

The failure of one or more major data centers or international or national cloud services can leave businesses, universities and anyone using the affected cloud service unable to access it. Due to the downsizing of local servers and the offloading of data to external data centers and data clouds, such an outage results in massive limitations to the organizations' business operations and the effectiveness of your business continuity plans.

3.5 Pandemics

As the corona pandemic has shown, a global pandemic has the potential to bring the entire global economy to a standstill, for example due to staff shortages, such as high sickness rates, curfews and the locking down of entire cities or regions. Particularly critical in this context are the service sectors as well as technology and logistics. Disruptions in these areas can have far-reaching effects on all critical infrastructures and can bring about production stoppages and resulting supply bottlenecks, particularly in the area of hardware and fuel supply. Looking at telecommunications networks, a supply bottleneck can mean that necessary spare parts to maintain the networks cannot be supplied

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

can be. This may result in a temporary reduction in the performance and availability of the telecommunications networks.

3.6 Willful destruction, manipulation, attacks, armed conflicts, sabotage and espionage

Due to the wide range of possible scenarios and their effects, further case distinctions were made. It is possible that the scenarios presented may occur in combination. In such a case, chain reactions can result in the area of the damaging effects, which multiply the damage potential.

3.6.1 Willful destruction, manipulation, Sabotage

By means of deliberate destruction, manipulation or sabotage, it is possible to destroy or impair the proper functioning of the telecommunications infrastructure at one or more points. Examples include the disconnection or destruction of cables and nodes or the damage or destruction of components or equipment of telecommunications networks. Since this is a case of wanton destruction, multiple actions, coordinated both in terms of time and region, must be expected if resources are available. In the case of long-distance connections, for example, there are only a very small number of physical cable systems (dark fiber), which are used by a large number of service providers. Because of this, these are targets with particularly far-reaching effects, for which increased georedundancy measures (see Section 4.1.4.) must be taken. Depending on the severity of the intervention, lasting disruptions in the telecommunications networks and services may occur until the affected hardware is replaced.

3.6.2 Warlike confrontation, attacks

Targeted air or ground attacks on telecommunications infrastructure in the course of a military conflict may cause lasting damage to the infrastructure. The continuation of hostilities in the affected areas or on the access routes may temporarily prevent the affected objects from being repaired. In such a scenario, other influencing factors such as a widespread power failure may also have to be taken into account. Furthermore, it must be taken into account that technical developments such as drones make highly precise, targeted attacks against infrastructures possible, even for non-state actors such as terrorist groups or individuals.

3.6.3 Espionage

The proper functioning and availability of telecommunications networks and services can be indirectly impaired by espionage. The consequences of espionage can include, for example, wanton destruction and manipulation (Section 3.6.1). Espionage is possible not only by external parties such as intelligence services of other countries, but also by internal forces such as employees of telecommunications companies or their suppliers. Consequently, protective measures should be comprehensive and designed in every conceivable direction.

3.6.4 Electromagnetic pulse (nuclear and non-nuclear)

An electromagnetic pulse can lead to the failure of unprotected electrical and electromechanical devices as well as to a power failure of undetermined duration. An electromagnetic pulse can be caused by an unnatural cause (e.g. an explosive device) or by a natural disaster (e.g. a nuclear explosion).

solar storm) can be considered. Restoring infrastructures after an electromagnetic pulse is very costly, since in the worst case all equipment must be replaced from scratch. The larger the electromagnetic pulse, the more likely that restoring function is equivalent to rebuilding any electronic infrastructure due to the extent and scope of the damage.

3.7 Above and beyond cyberattacks

Targeted and massive cyberattacks on critical basic infrastructure can have devastating consequences for the economy and public safety. They fundamentally threaten all businesses. Examples of these attacks are targeted ransomware attacks, which can restrict access to data and systems, or massive distributed denial of service (DDoS) attacks against individual services or facilities. Another possible scenario that is already active is "Expect-the-breach." This is based on the assumption that cyber espionage, especially by state or state-supported groups with sufficient time, financial, human and technical resources, begins well before a warlike conflict and that all networks have already been compromised as part of cyber espionage. In this context, eavesdropping on or reading data traffic (in the case of encrypted communications, especially metadata or decryption) can be a primary goal of such actors in order to gain information and, if necessary, prepare for later sabotage.

4 Derivation of possible measures

The corona pandemic and the associated exceptional situations have highlighted the great importance of high-performance digital networks and infrastructures. Digital technologies have helped sustain economic, political and social life. The operators of digital infrastructures and the telecommunications and Internet industries are also highly system-relevant for keeping other industries running.

The industry and digital infrastructure operators could therefore be consistently classified and recognized as systemically important to ensure that service providers, security personnel, and technicians have access to their sites of operation, even in the event of contact closures or restrictions, and that their ability to function can be maintained.

In addition to safeguarding against future crises and strengthening resilience, additional measures are needed to maintain functionality and operations in the event of a crisis. Against the background of the threat scenarios described in Chapter 3, the Federal Network Agency has worked with the Federal Office for Information Security, telecommunications providers and associations to identify measures that can improve the resilience of telecommunications networks in the future.

As a result, it can be stated that, from the point of view of the Federal Network Agency, the Federal Office for Information Security and the private sector, a reliable power supply is indispensable for the operation of telecommunications networks, since a failure of the power supply represents the greatest threat to the networks. In the event of a crisis, the power supply must be guaranteed for both mobile networks and fixed networks in order to enable communications services. In this context, it is pointed out that network operators already have emergency power and backup power systems on a voluntary basis. However, for technical reasons, these are only operational for a limited time, as for example accumulators have to be recharged and power generators supplied with fuel. Beyond securing the energy supply, however, further measures are needed to ensure the functionality of the mobile communications as well as the fixed network infrastructures.

For technical reasons, mobile communications technology generally enables the population to be provided with a wider range of telecommunications services in disaster situations, since the "last mile," i.e., the path between the transmission tower and the terminal, is bridged wirelessly. Mobile terminals are also widely used and have an integrated rechargeable battery, which enables communication without an external power supply, at least for a limited time. Another advantage of mobile networks is their cell broadcast functionality, which can be used to send warnings to terminals in disaster situations. Functioning cellular networks are therefore particularly important when considering the resilience of telecommunications networks.

Fixed networks are to a large extent the basis for modern mobile networks, since mobile data is transmitted over most of the distance in the transport and core network of the network operators. Fixed networks are therefore an indispensable part of measures to increase the resilience of telecommunications networks. Fixed networks can also themselves make an important contribution to ensuring communications in certain disaster situations. For example, it is conceivable that frequency ranges in which mobile communications networks operate may be disrupted and thus not available to the extent required. In such cases, it is important to be able to fall back on a resilient fixed network.

4.1 Technical Measures

The technical measures described below can help to improve the resilience of telecommunications networks and thus the availability of telecommunications services. Some technical measures can be implemented independently, while others may require the implementation of further measures or can only be implemented in combination with organizational measures (Section 4.2).

4.1.1 Emergency power for telecommunications networks and basic service offering in crisis situations

A disruption or failure of the power supply usually affects the functioning of the telecommunications networks immediately. The consequence is that telecommunications services can only be used to a limited extent or not at all. As a rule, it is no longer possible to make emergency calls in the event of a power failure. Cell broadcast technology, which in the future is to warn the population of dangers via mobile communications networks, also only works if a mobile communications cell is available in which the user's mobile device can log on. One of the most important measures for increasing the resilience of telecommunications networks is therefore to equip the telecommunications network infrastructure relevant for operation with backup power supply systems and technology for uninterruptible power supply.

Today, telecommunications network operators and telecommunications service providers already have a large number of such systems, often including mobile technology, which can be brought to crisis areas in a timely manner. However, these emergency power solutions, which are financed by the companies themselves on a voluntary basis, only help in the event of local and regional incidents; otherwise, such systems must be kept available throughout the country and require appropriate financing. Also, especially in the first few hours of a power blackout, there is no continuous telecommunications network, because permanently installed emergency power solutions are only available at limited technical locations of the network operators. If there are supraregional, long-lasting power failures, large-scale disruptions in the telecommunications networks are to be expected.

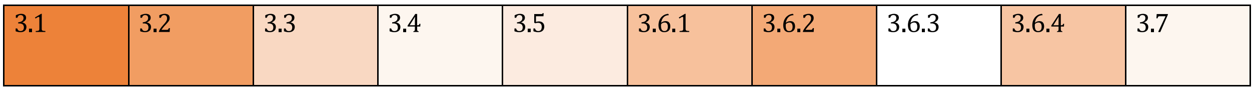
Against this background, the Federal Network Agency is proposing the measure of establishing uniform nationwide regulations for the emergency power supply of telecommunications networks.
In the future, citizens should be able to use a certain range of basic services even in the event of a widespread power outage, for example, to make emergency calls or receive warning messages via cell broadcast.

In order to be able to establish a base network supply with mobile communications technology in the event of a widespread power outage, the Federal Network Agency believes that not every base station necessarily has to have permanently installed emergency power technology. The network operators involved in drawing up the strategy paper have also indicated that not every technology site can be equipped with an emergency power supply, for example for fire protection reasons or because the statics do not permit this. However, in the view of the Federal Network Agency, equipping a certain proportion of base stations may be sufficient to supply the population with a base network.

In addition, the Federal Network Agency believes that further technical measures are conceivable to improve the coverage of mobile networks in the short term. If necessary, network operators could, for example, indicate an increase in transmission power limited to the time of the disaster situation. In this way, the transmission range can be increased by increasing the transmission power. However, it should be noted here that it is typically not the transmitting power of the base stations that is the limiting factor, but that of the terminal equipment. According to experts, however, this type of measure must be taken with particular caution, as increasing the transmission power must not disrupt other existing communication paths.

Another measure could be to restrict mobile network operation to low-band spectrum (700 to 900 MHz), which has a longer range for physical reasons. This could reduce the energy consumption of the networks. As long as only a limited (emergency) power supply is available, such a measure can extend the maintenance of mobile communications coverage over time.

As a result of the limited technical performance and capacity of a basic mobile communications network for disaster situations, however, the range of services on offer is severely restricted compared with ordinary mobile communications networks. Data-intensive applications that require high capacity and performance in the telecommunications network may not be usable in this case, or only to a very limited extent.



3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Figure 1 Extract from the mapping matrix for the measure Emergency power for telecommunication networks and basic service provision in crisis situations, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, civil unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage,
3.6.2 Warfare, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and

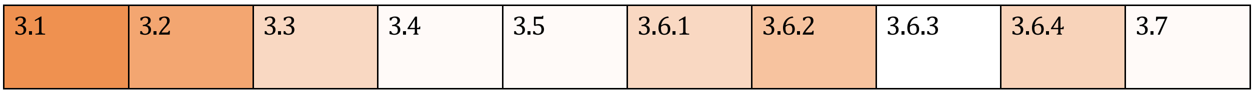
non-nuclear), 3.7 Above-normal cyberattacks. The darker the coloration, the stronger the correlation of the measure with the respective scenario was assessed.

4.1.2 Consideration of renewable energies for crisis prevention

The technical infrastructure of telecommunications networks depends on a reliable power supply. To bridge power outages, network backup systems are generally used today that are battery-based or run on fossil fuels. In order to minimize dependence on a regular fuel supply in the event of a crisis, network operators, associations and authorities believe that the use of renewable energies for technical sites should be increasingly considered in the future.

In the future, mobile communications sites could, for example, be equipped with battery systems in conjunction with photovoltaic modules or with fuel cells to ensure a limited supply of energy in an emergency. In the same step, however, the power consumption of the technology at the site would also have to be significantly reduced in the event of a crisis to ensure reliable functionality. This could be realized, for example, by reducing capacities and thus focusing on a limited range of services.

Operators of radio tower sites have already signaled their intention to use regenerative energy sources at more and more sites in the future, but are calling for improvements in the regulatory framework in this context.



3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Figure 2 Extract from the mapping matrix for the measure Consideration of renewable energies for crisis prevention, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage, 3.6.2 Warlike conflict, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear),
3.7 Cyberattacks above and beyond the normal level. The darker the color, the stronger the correlation between the measure and the respective scenario.

4.1.3 Examination of alternative site connections

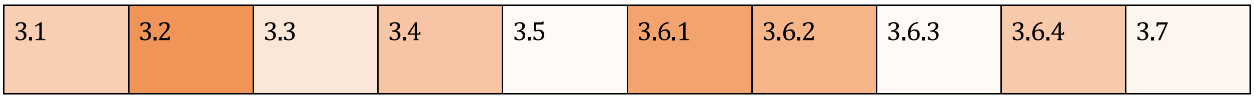
High demands are placed on modern mobile communications networks in terms of data rates, capacity and latency times. Reliability and fail-safety are also important factors. A high-performance connection of the transmitter sites in mobile communications networks to the core network of the respective provider is therefore nowadays usually implemented either via a fiber-optic cable connection or via a microwave link, as these technologies can best meet the requirements.

In disaster situations, too, the demands on the performance of mobile networks are very high. In particular, if the usually used connection of the respective mobile site no longer has the usual capacity or has even failed completely, a focus can be placed on basic functionalities such as cell broadcast, emergency call, telephony and possibly also limited Internet services. This focus allows the mobile network operator to consider site connectivity other than fiber and microwave in disaster situations.

One option already used in disaster situations can be to connect individual sites by means of directional radio links if the regular connection is no longer available. The Federal Network Agency has already made such short-term provisional radio relay connections possible in an unbureaucratic manner during the flood disaster in western Germany in 2021. Connecting sites via satellite can also be an adequate solution in individual cases to provide a basic service offering for mobile subscribers in disaster areas.

The examination of alternative site connections is primarily suitable for mobile networks, since a large number of users can be supplied simultaneously via mobile communications and the user's terminal equipment can still communicate for at least a limited time even in the event of a power failure due to integrated and external batteries.

In the fixed network, users' terminal devices are nowadays generally dependent on a constant power supply. The fixed network operators' technical sites close to customers are also often equipped with active technology, so communication via the fixed network is also not possible in the event of a power failure.
Nevertheless, in certain catastrophic cases, it may also make sense to examine alternative site connections in the fixed network area, for example via microwave radio.



3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Figure 3 Extract from the mapping matrix for the measure Examination of alternative site connections, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, civil unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage, 3.6.2 War, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear),
3.7 Cyberattacks above and beyond the normal level. The darker the color, the stronger the correlation between the measure and the respective scenario.

4.1.4 Improved georedundancy

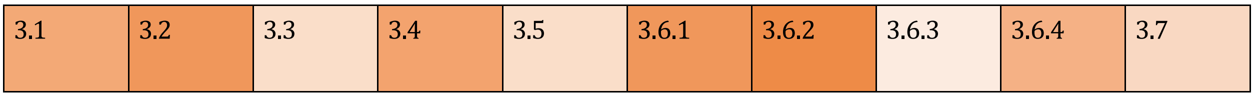
Even today, the principle of georedundancy - the geographical separation of technical infrastructure - is a widely used tool for increasing the resilience of telecommunications networks. For example, data traffic can usually be diverted to another connection without any problems if a particular infrastructure is no longer available at short notice. Network operators in Germany also often already have geo-redundant backup solutions in place for failures of central technical sites in order to minimize possible impairments to services5.

Against the backdrop of the threat scenarios presented in chapter 3 and the associated impact on the network infrastructure, an expansion of georedundancy is recommended. For important connections between nodes, both at the national and international level, the

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

Geo-redundancy will be strengthened to further improve the resilience of telecommunication networks with respect to the respective threats.

However, measures to strengthen geo-redundancy should not only focus on connections between network nodes and networks, but also on connections to the end customer.



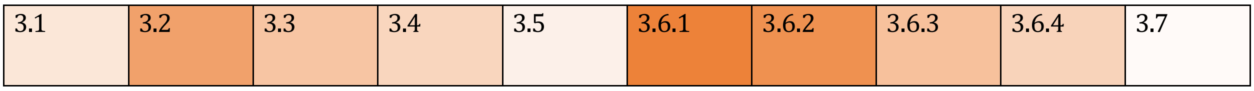
3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Figure 4 Excerpt from the mapping matrix for the measure Improved Georedundancy, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, civil unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics,
3.6.1 Willful destruction, tampering, sabotage, 3.6.2 Warlike confrontation, attacks,
3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear), 3.7 Cyberattacks beyond normal. The darker the coloration the stronger a correlation of the measure with the respective scenario was assessed.

4.1.5 Strengthen object protection (physical resilience)

Some of the scenarios presented in chapter 3 of this strategy paper pose a threat to the physical assets of telecommunications networks. For example, climate change with the accompanying increased natural disasters poses a threat to numerous locations, as demonstrated, for example, by the flood disaster in western Germany in July 2021.

To strengthen the resilience of telecommunications networks, even more effective protection of facilities (such as radio masts and technical sites) against these threats will be necessary in the future. Corresponding measures should be taken into account directly in the planning of the facilities and their locations.
One example of such property protection measures is extended protection against natural hazards as early as the planning and construction stages of such facilities, if possible on the basis of information and calculations that already take into account the current threats from increased natural disasters caused by climate change.



3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

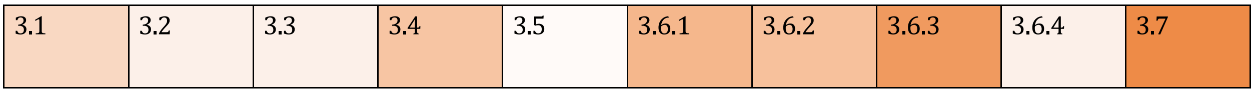
Figure 5 Extract from the mapping matrix for the measure Strengthen object protection (physical resilience), from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage, 3.6.2 Warlike conflict, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear),
3.7 Cyberattacks above and beyond the normal level. The darker the color, the stronger the correlation between the measure and the respective scenario.

4.1.6 Expansion of systems for attack detection and defense -

Telecommunications networks not only represent the crucial interface for cyber attacks, they are also themselves a target with particularly far-reaching implications for a large number of potential attackers. The chances of mitigating such attacks (on the networks and on subscribers) can be increased by an early and effective attack detection can be increased considerably. Network operators and service providers are already using systems for attack detection.

According to Section 8a, Paragraph 1a of the BSI Act (BSIG), operators of critical infrastructures are even obliged from May 1, 2023 to take appropriate organizational and technical precautions to prevent disruptions that are crucial to the functioning of the critical infrastructures they operate. This also includes the use of attack detection systems. These systems should be able to identify and prevent threats on an ongoing basis and to provide appropriate remedial measures for disruptions that have occurred. Accordingly, these systems should be taken into account when planning resource allocation.

In addition to the detection of attacks, the legislator has created the possibility in § 7c BSIG in conjunction with § 169 of the Telecommunications Act (TKG) to also prevent them by technical measures in order to avert significant threats. Among other things, these measures include the restriction, rerouting or prevention of data traffic to and from the relevant sources of interference. Telecommunications service providers must also provide the appropriate technical and organizational resources for this purpose.



3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Figure 6 Excerpt from the mapping matrix for the measure Expansion of systems for attack detection and defense, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, civil unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage,
3.6.2 Warlike confrontation, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear), 3.7 Above-normal cyberattacks. The darker the coloring the stronger a correlation of the measure was assessed with the respective scenario.

4.1.7 Expansion of backup solutions

Backups are a central technical measure to ensure the resilience of telecommunications networks. The operators of telecommunications networks and the providers of telecommunications services already have extensive and proven backup and restore strategies that are activated in the event of an emergency.

In the course of the threat scenarios presented in this strategy paper, especially with regard to possible cyber attacks of considerable magnitude, extensions of backup measures may be required. Institutions as well as industry demand measures against both physical and logical loss of a backup6.

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

Physical loss of the backup (examples):

- Theft, burglary, vandalism
- Fire, water damage
- Smoke and gas, dust and dirt
- Extreme temperatures
- Natural hazards caused by earthquakes, floods, avalanches

Logical loss of the backup (examples):

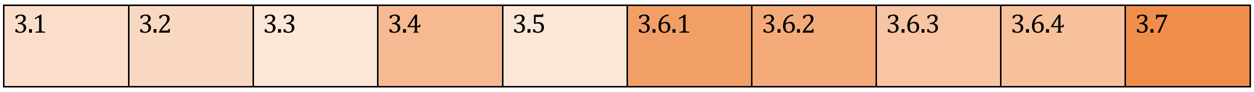
- The backup was deleted, e.g. by attackers
- Backup is compromised e.g. by infection of malware, ransomware or other malware that contains e.g. a backdoor
- Human error or intentional misconfiguration

Measures against physical loss of the backup (examples):
Implementation of the 3-2-1 backup strategy

- 3 backups
- 2 different storage media (in particular also use of read-only storage media, which cannot be overwritten by attackers)
- 1 copy at an external location

Measures against logical loss of the backup (examples):

- Complete organizational and personnel separation of system administrator and storage administrator (least privilege model and separation of duty)
- Backup employees must be security- or sabotage-certified (SÜG)
- Backup systems shall be classified according to their risk assessment and shall be hardened and protected to a special degree. In particular, multifactor authentication (MFA) is to be introduced.
- The backup system must be monitored by a Security Information and Event Management (SIEM) and an Endpoint Protection system.
- Online backups must be regularly checked for malware by a vulnerability scanner or sandbox
- Documented recovery tests must be performed on a regular basis



3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Figure 7 Excerpt from the mapping matrix for the measure Expansion of backup solutions, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, civil unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, tampering, sabotage, 3.6.2 Warlike confrontation, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear), 3.7 Cyberattacks beyond normal. The darker the coloration the stronger a correlation of the measure with the respective scenario was assessed.

4.2 Organizational Measures

In addition to a number of technical measures, the telecommunications network operators, associations and authorities involved in the strategy paper also identified organizational measures that can directly or indirectly improve the resilience of telecommunications networks.

4.2.1 Joint situation center of network operators and authorities

Telecommunications network operators, associations, the Federal Office for Information Security and the Federal Network Agency propose setting up a joint situation and response center for telecommunications network operators and the relevant authorities to improve cooperation between the various players in acute threat situations and to facilitate the coordination of measures[7].

Part of the situation center should be staffed around the clock with employees from the relevant network operators and authorities to assess the current situation of the telecommunications networks. The telecommunications situation center should be fed by information from all network operators and authorities and organizations (such as the Federal Agency for Technical Relief or even weather services) at the municipal, state and national level. This is intended to ensure that a comprehensive assessment of the current situation can be made so that the necessary measures to combat a particular disaster situation can be taken early and efficiently.

The situation center is to be established on a virtual as well as on a presence basis and prepared for crisis situations by means of regular exercises (cf. chapter 4.2.2).

The conditions should be created for the representatives of companies and authorities involved in the joint situation center to be able to work with each other's confidential information, for example through appropriate contracts and security checks. The protection of individual company and business secrets must be guaranteed at all times.

The management and coordination of such a situation center should be handled by an independent body with clearly defined responsibilities and powers. An existing federal authority could be designated for this purpose.

3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Figure 8 Excerpt from the mapping matrix for the measure Joint Situation Center of Network Operators and Authorities, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, civil unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage,
3.6.2 Warfare, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and

[7] The cybersecurity agenda of the Federal Ministry of the Interior and Homeland Affairs also pursues the same goal under item 5, "Strengthening the cyber resilience of critical infrastructures," as a measure for the 20th legislative period. Here, in particular, a dense connection of KRITIS operators to the BSI Situation Center is envisaged. To this end, a sector-specific Cyber Emergency Response Team (CERT) is to be established by the CRITIS operators for each CRITIS sector (see: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.html).

non-nuclear), 3.7 Above-normal cyberattacks. The darker the coloration, the stronger the correlation of the measure with the respective scenario was assessed.

4.2.2 Optimization of cooperation through exercises

The companies, associations and authorities involved in this strategy paper are in favor of regular exercises to safeguard telecommunications in crisis situations. The exercises should cover the scenarios outlined in chapter 3 and ensure the optimization of cooperation between telecommunications network operators, authorities and other stakeholders.

Such an exercise concept has already been established within the framework of the interstate and interdepartmental crisis management exercise (LüKEx) and has been successfully carried out several times in recent years.

However, it would seem sensible for such or comparable exercises in the future to involve not only government players but also critical infrastructure companies (CRITIS). In the view of the Federal Network Agency, nationwide but also regional telecommunications network operators should be included in such exercises. For example, many smaller telecommunications network operators have regionally very important fiber-optic infrastructures, which are just as important and worth preserving in the event of a crisis as the structures of large, supraregional providers. Furthermore, the providers and operators of 5G campus networks should also be involved in exercises in the future, depending on the respective scenarios. In many cases, 5G campus networks are networks of industrial production sites with high economic importance for the industry. It is also suggested that other sectors and critical infrastructures be included in the exercises in order to optimize interaction in the event of a crisis.

In connection with the aforementioned exercises, stress tests should also be increasingly conducted to check telecommunications networks for possible vulnerabilities.

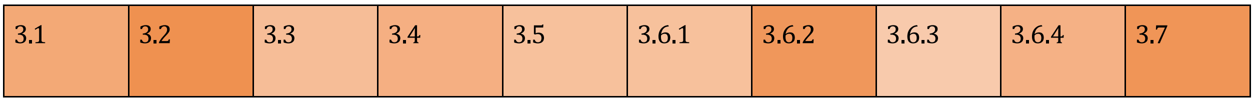


Figure 9 Extract from the mapping matrix for the measure Optimization of cooperation through exercises, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, civil unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage, 3.6.2 Warlike conflict, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear),
3.7 Cyberattacks above and beyond the normal level. The darker the color, the stronger the correlation between the measure and the respective scenario.

4.2.3 Ensuring communication between stakeholders in the crisis

An essential factor during crisis situations is not only internal but also the most efficient management of external communication (e.g., with authorities, media), which can be implemented by an established management of the situation center (cf. chapter 4.2.1).

In addition, individual measures must be taken in the respective organizations to ensure communication. Contact persons and responsibilities must be named and known, and communication channels must be regularly reviewed in the event of a crisis.

Between 2016 and 2017, the thematic working group Crisis Communication System investigated different communication systems that should still be available in the event of massive power and information technology or telecommunications failures. The aim was to establish a delineated, common system for the early detection of information technology crises and a common crisis management system with corresponding high-availability (communication) structures and processes for critical infrastructure companies and the responsible authorities.

At the plenary meeting of the Critical Infrastructures Implementation Plan (UP KRITIS) 01/2017, the decision was made to ask the Federal Ministry of the Interior and for Home Affairs for a decision in principle, with the involvement of the Federal Office for Information Security and the Federal Office for Civil Protection and Disaster Assistance, on the use, expansion and adaptation of the modular warning system (MoWaS). After the events in the 1st half of 2022 (esp. KA-SAT outage), possible technical solutions are to be examined again. In the view of the Federal Network Agency, this investigation can be re-examined and a deployment proposed.

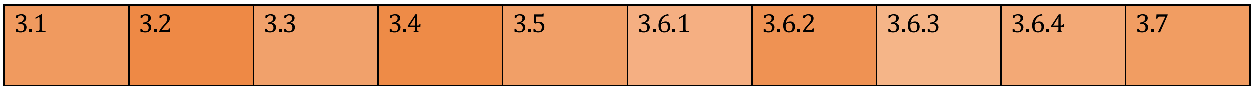


Figure 10 Extract from the mapping matrix for the measure Ensuring communication between actors in a crisis, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, riots, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage,
3.6.2 Warlike confrontation, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear), 3.7 Above-normal cyberattacks. The darker the coloring the stronger a correlation of the measure to the particular scenario was assessed.

4.2.4 Prioritization of energy supply in case of shortage

The prioritization of energy supply during a power shortage situation demanded by the industry and the safeguarding of telecommunications networks as critical infrastructure require clear political guidelines. In the event of a crisis, the supply of fuel to mobile and stationary network backup systems is a joint task for companies and authorities, as the companies themselves may not be able to gain regular access to this resource or transport to the point of use may not be possible.

At the same time, the necessary measures at the end-customer level must be considered in the context of a comprehensive understanding of the resilience of telecommunications networks. Just as food and water should always be stocked for a few days, it is also advisable for private households to have a mobile power supply (e.g., power bank) to ensure communications in the event of a disaster or crisis so that the batteries of mobile devices can be recharged even without an external power supply.

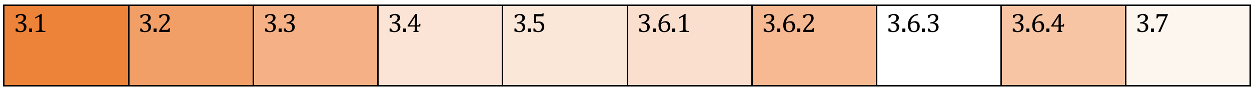


Figure 11 Extract from the mapping matrix for the measure Prioritization of energy supply in case of shortage, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage, 3.6.2 Warlike conflict, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear),

3.7 Cyberattacks above and beyond the normal level. The darker the color, the stronger the correlation between the measure and the respective scenario.

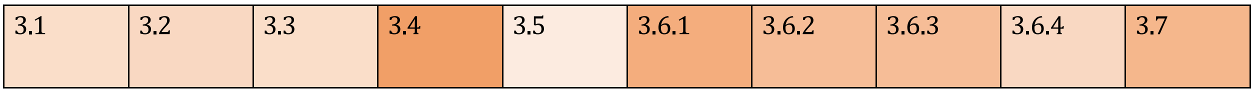
4.2.5 Vulnerability analysis in the area of network interconnection and network access

Interconnection with other networks creates additional vulnerabilities for telecommunications network operators, which can impair or prevent a network's ability to function and thus communication. The following measures can reduce this risk:

- Security aspects should already be taken into account when defining interfaces. Obsolete, insecure protocols should be replaced with secure products as quickly as possible. If this is not possible, the functional scope of the obsolete protocols should be restricted and increased monitoring of the network interconnection should be carried out.
- To ensure that access to collocation rooms can be made secure, clear and binding regulations have already been laid down for granting access permission. One minimum requirement is that access rights are linked to a single person. The access rights granted must be checked regularly and withdrawn if necessary. In addition, the regulations for granting access rights must be regularly checked for effectiveness, and contact persons must be defined for malfunctions and security incidents.
- Physical security is equivalent to that of the entire telecommunications network, and methods should be developed at the planning stage to conceal the network topology from the outside world.
- The information technology protocols should be secured between the partners in such a way that the integrity of the connection cannot be broken. In addition, there should be a physical separation between control and user data.

The following are proposed as measures to enhance resilience in network interconnections:

- Integration into the emergency power supply to maintain the quality of service
- Redundant connection to maintain the probability of failure according to the priority of the connection
- Monitoring traffic for anomalies and logging changes
- Integration with the attack detection system



3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

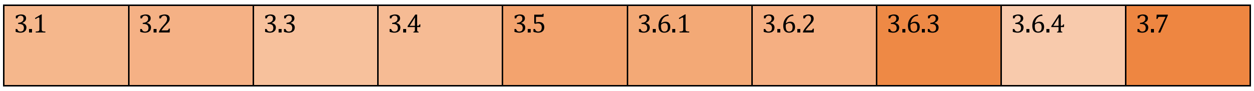
Figure 12 Excerpt from the mapping matrix for the vulnerability analysis measure in the area of network interconnection and network access, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, civil unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage, 3.6.2 Warlike confrontation, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear), 3.7 Above-normal cyberattacks. The darker the coloring the stronger a correlation of the measure was assessed with the respective scenario.

4.2.6 Employee training, best practices

When considering possible organizational measures to strengthen the resilience of telecommunications networks, the training needs of employees should be regularly reviewed. Here, it should be examined whether and to what extent it is also possible to expand the training and continuing education offerings for employees.

In particularly critical areas, a security check of the employees working in these areas is currently already required. The security requirements should be continuously put to the test and adjusted as necessary. In particular, in areas not classified as critical, a tightening of security requirements, e.g., access regulations to buildings, is recommended.

In addition, raising employee awareness and providing regular information about potential threats and security gaps are crucial to ensuring a higher level of security.
Regular checks and drills are an effective means of being able to assess the level of knowledge of employees, identify training needs at an early stage and organize any necessary follow-up training.



3.1	3.2	3.3	3.4	3.5	3.6.1	3.6.2	3.6.3	3.6.4	3.7

Figure 13 Extract from the mapping matrix for the measure Training of employees, best practices, from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, civil unrest, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, tampering, sabotage, 3.6.2 Warlike conflict, attacks, 3.6.3 Espionage, 3.6.4 Electromagnetic pulse (nuclear and non-nuclear),
3.7 Cyberattacks above and beyond the normal level. The darker the color, the stronger the correlation between the measure and the respective scenario.

5 Summary and Outlook

The Federal Network Agency recommends that the digital infrastructure in Germany be expanded in a resilient and sustainable manner. This strategy paper identifies areas for action and concrete measures to increase the resilience of telecommunications networks and services. These were developed jointly with the industry. There is agreement in the industry and the authorities to cooperate in the implementation of measures.

In view of the measures presented, the first step should be to determine which of these measures should be prioritized for implementation. When clarifying the feasibility of measures, a large number of follow-up questions must be addressed. For example, required and defined technical and organizational measures must be adapted within the framework of proportionality according to the needs and size of the respective companies; not every company will be able to implement every measure equally quickly and comprehensively, while other companies may already have implemented some of the measures.

Further steps should determine which of the technical measures described should be implemented in the networks. This also applies with a view to feasibility in terms of timing and the cost bearing. The same applies to the organizational measures described above, for which responsibilities and procedures in particular must be defined. Finally, legal foundations must also be created if necessary.

In addition to achieving the best possible individual resilience for each telecommunications network or service, it is also important to develop and pursue a cross-network strategy. As described above, in the event of crises and disasters it is necessary to consider the entirety of the affected telecommunications infrastructures (mobile communications and fixed network).

Some of the measures outlined in this strategy paper, such as the joint situation center of network operators and authorities (cf. Section 4.2.1), also require the active cooperation of companies, associations and authorities and require further specification with regard to their responsibilities and specific design.

Financial and legal aspects must also be clarified as part of the implementation of measures.

The Federal Network Agency suggests continuing the industry dialog between the companies, associations and authorities involved as a further step. The aim is to determine the feasibility of the measures outlined and to define responsibilities. Resilient and strong networks maintain everyone's ability to act, even and especially in times of crisis, and thus create the first opportunity to efficiently face and master the respective challenges.

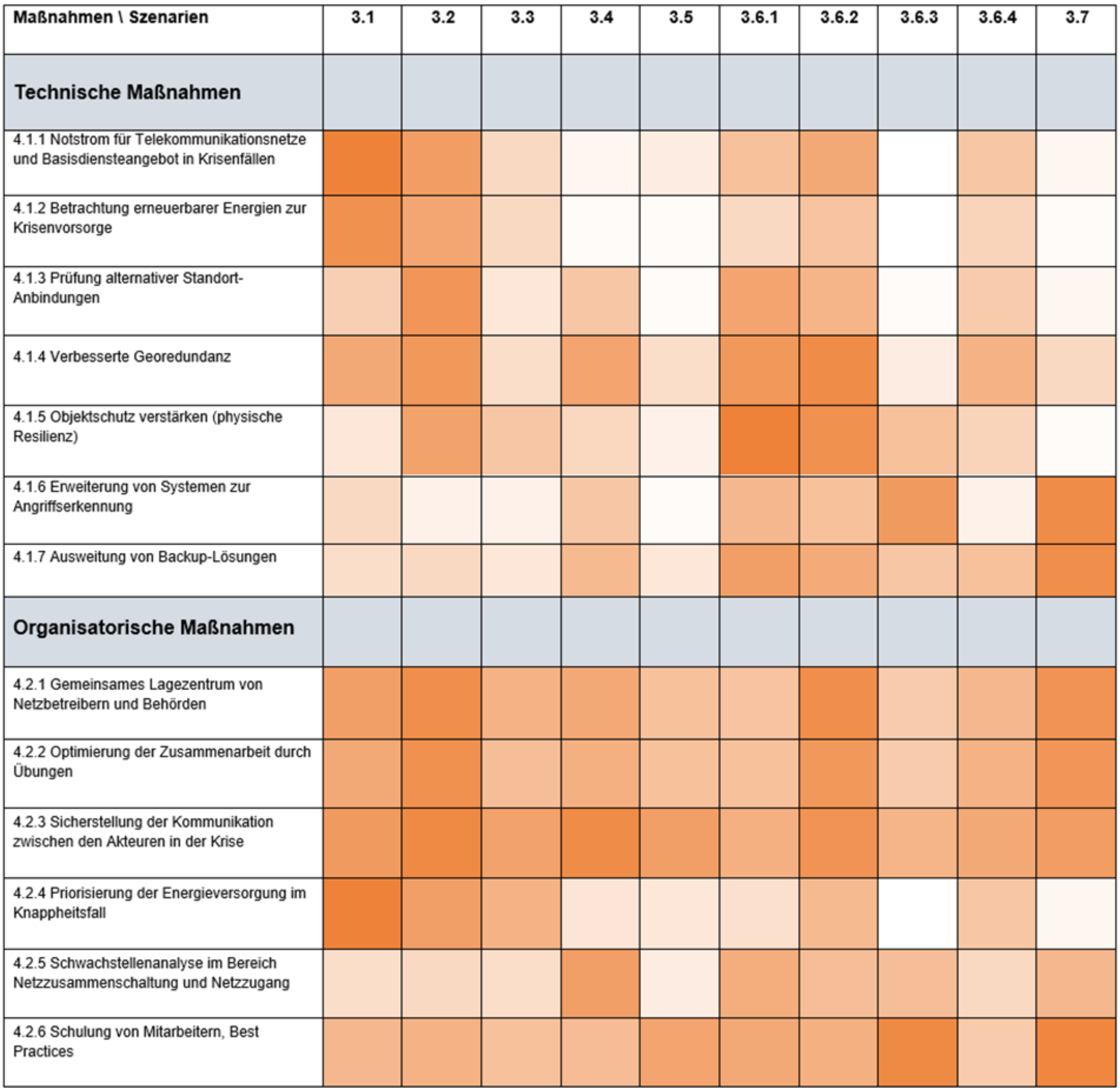
6 Appendix

6.1 Participating companies, associations and authorities

- 1&1 AG
- ANGA the broadband association
- Federal Office for Information Security
- Federal Ministry for Digital Affairs and Transport
- Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway
- German Broadband Communications Association (BREKO)
- German Association of Energy and Water Industries (BDEW)
- German Federal Association for Fiber Optic Connections (BUGLAS)
- German Association for Information Technology, Telecommunications and New Media (BITKOM)
- German Telekom AG
- Telefónica Deutschland Holding AG
- Association of Telecommunications and Value-Added Service Providers (VATM)
- Association of Municipal Enterprises (VKU)
- Association of the Internet Industry (eco)
- Vodafone GmbH

6.2 Mapping Matrix

The matrix represents the unweighted and averaged assessment of the relationship between measures and scenario by 1&1 AG, the Federal Office for Information Security, the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway, the German Association of Energy and Water Industries, Deutsche Telekom AG, OneFiber Interconnect Germany GmbH, the Association of Municipal Enterprises, the Internet Industry Association and Vodafone GmbH. The darker the color, the stronger the correlation between the measure and the respective scenario.



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										

Figure 14 Mapping matrix of scenarios and measures, scenarios from left to right: 3.1 Disruption of energy supply, 3.2 Natural disasters, exceptional climatic conditions, 3.3 Economic difficulties, riots, 3.4 Failure of central Internet infrastructures, 3.5 Pandemics, 3.6.1 Willful destruction, manipulation, sabotage, 3.6.2 Warlike conflict, attacks, 3.6.3 Espionage,

3.6.4 Electromagnetic pulse (nuclear and non-nuclear), 3.7 Above-normal cyberattacks. The darker the coloring the stronger a correlation of the measure with the respective scenario was assessed.

List of Figures

Imprint

Publisher

Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway
Tulpenfeld 4
53113 Bonn

Source of supply | Contact person

Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway Press Office
Tulip field 4
53113 Bonn
pressestelle@bnetza.de
www.bundesnetzagentur.de

Booth

August 2022

Print

Federal Network Agency

Image credits

Title: AdobeStock, vectorfusionart

Text

Unit 217