Federal Office
of Civil Protection and
Disaster Assistance

BBK

10 years of the "CIP Strategy"

Insights into the implementation of the
National Strategy for Critical Infrastructure Protection (CIP Strategy)

Expert Information

Working practice in civil protection

Volume 21

BBK. Working together. Living in safety.

10 years of the “CIP Strategy”

Insights into the implementation of the National Strategy for Critical Infrastructure Protection (CIP Strategy)

Publisher:

Federal Office of Civil Protection and Disaster Assistance (BBK)

In collaboration with:

Federal Office for Information Security (BSI)
Federal Financial Supervisory Authority (BaFin)
Federal Office for Agriculture and Food (BLE)
Federal Agency for Technical Relief (THW)
Federal Institute for Research on Building, Urban Affairs and Spatial Development (BBSR), part of the Federal Office for Building and Regional Planning (BBR)
Federal Ministry of Finance (BMF)
Federal Ministry of the Interior, Building and Community (BMI)
Federal Ministry of Education and Research (BMBF)
Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)
Federal Ministry of Transport and Digital Infrastructure (BMVI)
Federal Ministry for Economic Affairs and Energy (BMWi)
Federal Network Agency (BNetzA)
Conference of National Cultural Institutions (KNK),
Guidelines for the protection of cultural property (SiLK)
Office of the National Focal Point for the Sendai Framework (NKS) at the BBK

Compiled on:

February 2020

Disclaimer: This expert information was translated to the best of our knowledge. In order to make the expert information generally intelligible, the text includes official and unofficial translations of German federal agencies, laws, regulations and literature. Whenever possible, the official translation has been used.

Contents

Foreword

Christoph Unger
President of the German Federal Office
of Civil Protection and Disaster Assistance

Dear reader,

“In Germany, the supply of energy, IT and transport services, drinking water and many other vital facilities to the public and companies is very good. The safety and security standards and the reliability of critical infrastructures are at a high level. However, in view of some new and some growing dangers, we cannot be satisfied with what we have achieved so far.

International terrorism, natural disasters as well as increasingly complex technologies pose challenges over the long term.

These were the words of the former Federal Minister of the Interior, Dr Wolfgang Schäuble, when the National Strategy for Critical Infrastructure Protection was passed into law by the German cabinet on 17th June 2009.

This statement largely remains true to this day: even though supply security in Germany continues to enjoy a leading position internationally – not least due to high security standards – we continue to face great challenges in view of terrorist and hybrid threats, climate change, and systematic increases in complexity resulting from digitalisation. We cannot take our foot off the pedal.

There have also been a host of changes in this field over the past 10 years. Critical infrastructure protection has been adopted as one of the central tenets of domestic security and has become a cornerstone of civil protection and the safeguarding of people’s livelihoods. This can be seen, for example, in the fact that measures designed to protect critical infrastructure have been passed as legislation and that the term ‘critical infrastructure protection’ is increasingly used.

The institutionalisation of shared structures between the responsible departments at the national level and between the federal government and the German states can be viewed as a milestone. Recent years have seen a growing realisation that critical infrastructure protection is an issue requiring coordinated cooperation across departments and levels, evidenced in cross-departmental working groups at the federal level, as well as in an established cooperation between the federal and regional governments. Supported by the public-private partnership between the state and private operators as part of UP KRITIS, critical infrastructure protection in Germany incorporates a system of cooperative relations between the key actors of which all parties can be proud.

The concept of critical infrastructures has also developed in terms of methodology: from the distinction between the physical protection of stationary plants and IT security in networks to an integrated protection system; from a plant-focused perspective to a more systematic approach; from critical infrastructures as a starting point to critical services – it has been a long, sometimes convoluted and occasionally difficult yet ultimately rewarding journey.

This report on the implementation of the National Strategy lays out many, though not all, of the results achieved through this work on critical infrastructure protection. It begins before the National Strategy was passed into legislation, with some of the very first – “strategy-less” – steps towards critical infrastructure protection, and uses examples to elucidate how the comprehension of and approach to critical infrastructure protection in Germany has developed over the years.

In light of the range of measures documented here, the prediction made by the Federal Minister of the Interior back in 2009, namely that the strategy would “have a positive impact on the fundamental thought processes, actions, and behaviours in all security and policy issues concerning critical infrastructure protection”, has proven prescient.

A number of different authorities from a range of departments have made important contributions to this report. It would not have been possible to compile this documentation without their involvement, their work in the field of critical infrastructure protection, and their willingness to report back on this work.

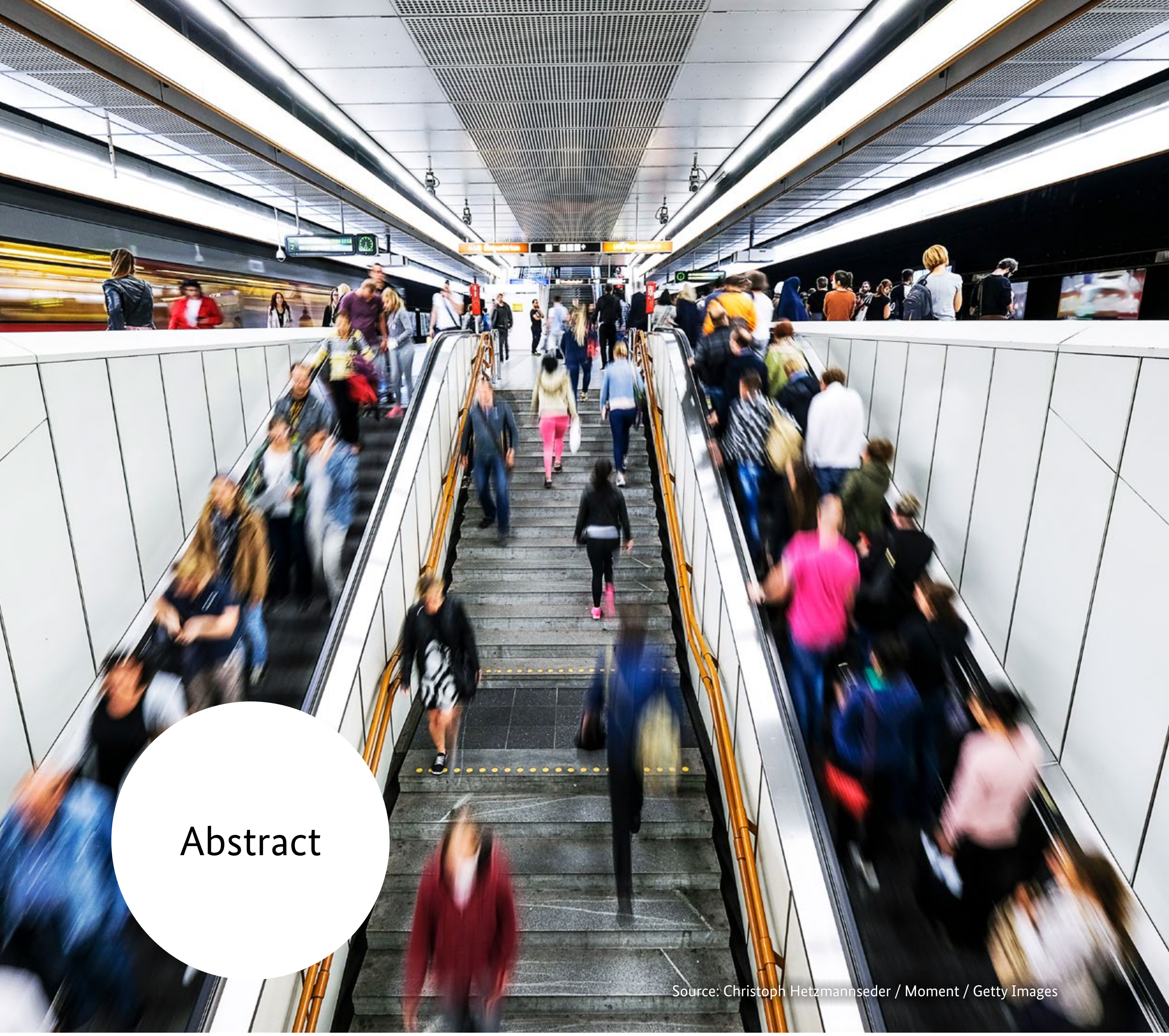
I would like to take this opportunity to express my deep gratitude for this collaboration between authorities and departments, which in itself further highlights the cross-departmental and cross-sectoral character of critical infrastructure protection.

This initial document is intended to be a federal report. My personal wish is that structural developments in critical infrastructure protection can be incorporated in the future, with the federal and state governments jointly reporting on progress made in critical infrastructure protection.

As for now, I sincerely hope that you enjoy reading this report.

Bonn, February 2020

Christoph Unger



Abstract

Source: Christoph Hetzmannseder / Moment / Getty Images

The origins of critical infrastructure protection in Germany (→ Chapter 1.1)

The first measures to protect critical infrastructures in Germany were taken at the end of the 1990s. The establishment of the cross-departmental "AG KRITIS" working group by the Federal Ministry of the Interior (BMI) in 1997 did not just represent a first organisational structure for critical infrastructure protection; it also marked the introduction of the German acronym "KRITIS", which stands for "Kritische Infrastrukturen" or "critical infrastructures" (CI) and which is still in use to this day. A year later, the first department dedicated to critical infrastructure protection was created within the Federal Office for Information Security (BSI). Over the next few years, the focus of this new area of policy was widened, both conceptually and in terms of content: critical infrastructure protection was not just intended to focus on IT security issues, but would also incorporate a broader approach to threats. This led to the founding of the Federal Office of Civil Protection and Disaster Assistance (BBK) in 2004, to provide a further organisational unit for critical infrastructure protection within a federal ministry. A series of methodological instruments emerged over subsequent years, including the "Baseline Protection Concept" (BMI 2005a; → Infobox 1) and "Protecting Critical Infrastructures – Risk and Crisis Management: A guide for companies and government authorities" (latest version: BMI 2011a; → Chapter 2.1.1). The "National Plan for Information Infrastructure Protection" (BMI 2005b) served to highlight aspects of the programme, along with the "Federal Implementation Plan" for government authorities and the "CIP Implementation Plan" for operators of critical infrastructures (BMI 2007a).

A strategic framework: the "National Strategy for Critical Infrastructure Protection (CIP Strategy)" (→ Chapter 1.2)

In 2007, work began on setting out a comprehensive strategic foundation for critical infrastructure protection. This led to the passing of the "National Strategy for Critical Infrastructure Protection (CIP Strategy)" (BMI 2009) by the federal cabinet in 2009. On the one hand, the strategy was intended to provide a framework for the tried and tested approaches already in use, while also highlighting the need for further development and expansion. The strategy identifies future challenges, in particular with regard to society's growing dependence on increasingly interlinked infrastructure systems and an evolving landscape of new terrorist threats and natural disasters. With this in mind, the strategy conveys the importance of focusing on a broad array of critical infrastructures as well as on a wide range of threats.

The "All-Hazards Approach", which links IT security aspects with so-called "physical protection", thus forms a core element of the CIP Strategy. The focus on all phases of risk and crisis management, as set out in the "CIP Implementation Plan" (BMI 2007a), occupies an equally prominent position. The strategy is shaped by a "cooperative approach" as a form of collaboration between the state and private industry, and by the priority given to voluntary self-commitment on the part of industry rather than to statutory regulation. During the drawing up of the CIP Strategy, the federal and regional governments discussed how to classify the critical infrastructure sectors. The resulting list of sectors agreed upon by the federal and regional governments was not published as part of the strategy itself but is nevertheless closely linked to it (→ Infobox 2). The CIP Strategy is more a guide than a fixed set of rules for critical infrastructure protection in Germany. The strategy does not provide detailed descriptions of individual steps; rather, the intention was that these steps would be set in place during the implementation phase. The following chapter of the Implementation Report provides some insights into this process (→ Chapter 2).

The development and implementation of methodological principles (→ Chapter 2.1)

Methodological principles are courses of action for specific groups and areas of application and thus perform various functions within the context of critical infrastructure protection. They serve to give substance to an area of discussion, to help formulate the expectations placed on individual groups of actors, to structure the co-operation between these actors and to build links to established procedures. Some are incorporated in binding directives or formal instruments; others serve purely as orientation. Methodological principles start to have an impact as early as the development phase: they force those involved to grapple more intensely with the topic in question and have often acted as the starting point for cooperation between actors.

The operators of critical infrastructures – whether companies or authorities – are responsible for ensuring the secure and reliable operation of their plants and facilities. To help achieve this, the guide entitled "Protecting Critical Infrastructures – Risk and Crisis Management. A guide for companies and government authorities" (BMI 2011a) represents a key instrument for critical infrastructure protection (→ Chapter 2.1.1). The methodology presented in this guide is based on recognised standards which have been tailored to critical infrastructure protection in close concert with operators. In addition, a series of industry-specific guides, as well as a procedure for structured collaboration between operators and state authorities for risk and crisis management, have been compiled (→ Chapter 2.5.2 and Chapter 2.5.4).

To ensure that operators of critical infrastructures are aware of their special responsibilities and that state bodies can find the relevant contacts within the private sector, a methodology for identifying critical infrastructures has been developed and published as a guide (BBK 2019a, → Chapter 2.1.2). As the issue of whether or not a particular plant or facility is considered to be critical depends on the approach, the methodology described here can be adapted to suit the respective context in which it is being applied. One application at the federal level is the identification of critical infrastructures within the meaning of the *IT Security Act,* which is governed by the *BSI Critical Infrastructure Ordinance (BSI-KritisV)* (→ Infobox 16). The Hague Convention identifies a cultural property as something that especially reflects the identity of communities (→ Infobox 3). The national risk analysis for civil protection investigates the impact that different risk events would have on the population and its basic needs (→ Chapter 2.1.3). The consequences of storms or pandemics are, for example, largely dependent on the degree to which they impact critical services (cf. BT-Drs. 17/12051; BT-Drs. 18/208). As such, once the scenario has been stipulated in the risk analysis, the next step is to investigate the impact on critical infrastructures, so that the effects can be viewed as a whole. The failure of critical infrastructures as an "indirect" consequence of an event hence occupies an important position in the methodology for risk analysis in civil protection.

The potentials of regional planning for risk prevention were examined in a "demonstration project of spatial planning", paying special attention to the concerns of critical infrastructures (cf. BMVI/BBSR 2015). With its spatial approach to risk management, spatial planning offers a cross-sector perspective on critical infrastructure protection. It can highlight where a focus on individual, industry-specific safety regulations falls short or would stand in the way of a holistic solution, for instance due to the spatial proximity of different infrastructures. Suitable methodological principles need to be developed in order for stakeholders to be able to use the opportunities presented by preventative risk management, for example in regional planning (→ Chapter 2.1.4). Considerations about dealing with critical infrastructures have been incorporated in the "Handbook for the design of flood prevention in spatial planning" (cf. BMVI 2017; → Infobox 4).

The operational framework for critical infrastructure protection (→ Chapter 2.2)

According to the CIP Strategy concept, "either – primarily – as a moderator or – if required – by rule-making, the state regulates the measures for safeguarding and securing the overall system and the system's procedural flows" (BMI 2009, p. 2). In line with this key concept, critical infrastructure protection has, and continues to focus on, non-regulatory instruments.

There is no comprehensive "law governing critical infrastructure protection" in Germany. Despite this, certain aspects of critical infrastructure protection have made their way into specialised laws over time (→ Chapter 2.2.1), whether to convey regulations from the European level into German law or to meet a recognised need for regulation at the national level. The legal regulations with an explicit link to critical infrastructure protection have a number of forms and functions: in some cases they formulate abstract objectives, stipulate the powers of authorities or lay out specific requirements for operators. In particular the *IT Security Law,* which came into force in 2015, has left its mark on many specialised laws as an overarching piece of legislation. It made it necessary to regulate aspects of its implementation through the use of sub-legislation and also set in motion the development of standards for legally compliant implementation. The *Energy Industry Act* shows how the general legal framework for critical infrastructure protection is linked with subject-specific regulations (→ Infobox 5).

Norms and standards are used to formulate legal stipulations in specific terms, particularly with regard to a rather abstract "state of technology", which laws often refer to. They also perform this function in the context of critical infrastructure protection (→ Chapter 2.2.2).

They are used in one form or another in all sectors of critical infrastructure systems, include technical specifications and describe approaches or organisational processes. Many norms and standards generally aim to provide reliable and safe processes; some also expressly relate to critical infrastructure protection. Yet it is not just the passed norms and standards that have an effect; their development can lead to new topics being revealed by experts as part of the structured process, in order for common positions to be agreed upon.

Long before "critical infrastructure protection" had become an established area of policy, the safeguarding of central utility services in defined crisis situations formed part of statutory regulations (→ Chapter 2.2.3).

Precautionary laws feature provisions for coping with supply shortages in peacetime, while safeguarding laws are designed to deal with supply crises in situations of tension or defence (Art. 80a or 115a GG). The areas of supply addressed in these laws partly correspond to the sectors of critical infrastructure systems. One example of a legal norm, which addresses supply crises in both peacetime and in situations of tension or defence, is the combined *Emergency Food Control Act* and the *Emergency Food Supply Act,* amended in 2017 (→ Infobox 6).

Critical infrastructure protection as a cross-sectoral issue (→ Chapter 2.3)

Critical infrastructure protection overlaps with other policy areas in many ways due to both the wide-ranging nature of the topic across all nine sectors and to the All-Hazards Approach. As a result, aspects of critical infrastructure protection can also be found in other strategic policy documents and are addressed there within their respective contexts (→ Chapter 2.3.1). Some of the relevant strategies focus on areas that are impacted by different types of threat. For example, the "Cyber Security Strategy for Germany" (BMI 2016a) focuses on cyber threats (→ Infobox 7), while the "German Strategy for Adaptation to Climate Change" (BReg 2008) looks at the impact of climate change (→ Infobox 8). Others detail the approach for critical infrastructure protection within a sector, for example the "Security Strategy for the Freight Transport and Logistics Industry" (BMVI 2014, → Infobox 9). The United Nations' "Sendai Framework for Disaster Risk Reduction" covers a wider perspective (NKS 2019): it incorporates the full range of threats in line with the All-Hazards Approach and addresses critical infrastructure protection as part of disaster prevention for society as a whole (→ Infobox 10).

The "Civil Defence Concept" (BMI 2016b) maps out the civil dimension of the overall defence concept. In other words, it focuses on threats that could occur in conjunction with armed conflicts and hybrid threat situations (→ Chapter 2.3.2). Aspects of critical infrastructure protection are an integral part of the concept and therefore arise at various points. By way of example, requirements for maintaining state and government functions can be understood as threat-specific measures for critical infrastructure protection in the *state and administration* sector (→ Infobox 11).

To be able to promote the advancement of scientific knowledge for the benefit of critical infrastructure protection, a pillar from the "Research for Civil Security" framework programme has been dedicated to the topic (BMBF 2018, → Chapter 2.3.3). Operators, such as authorities and organisations with a security remit or operators of infrastructure companies, are closely involved in all the research projects to ensure that any solutions developed are practicable and fit for purpose. Furthermore, societal, legal and ethical questions are considered from the outset (→ Infoboxes 12, 13 and 14). The federal government's research framework programme on IT security promotes research projects in the field of critical infrastructure protection, which are specifically linked to IT security (ITS|KRITIS, → Infobox 15).

Critical infrastructure protection – a task requiring cooperation between various actors (→ Chapter 2.4)

The CIP (Critical Infrastructure Protection) Strategy (BMI 2009, p. 12) states that "in order to strengthen critical infrastructure protection, the requirement is for intensive cooperation, coordination and information between and among the relevant partners and players". This is due to the highly diverse range of actors involved in critical infrastructure protection: responsibilities are shared between operating companies and state bodies; technical jurisdictions are spread across various departments; supervision is conducted by authorities at various administrative levels; the operators of critical infrastructures are organised in a number of different associations; different research institutes focus on various aspects of protecting critical infrastructures – and this does not even begin to cover the many groups of actors listed under "cooperative approach" in the CIP Strategy (→ Chapter 1.2). Over time, those involved have fulfilled the mandate to work together in a variety of ways.

Critical infrastructure protection is viewed as a collective national task. Cooperation between federal government and state bodies plays a pivotal role and the creation of associated structures is a key step forward in implementing the CIP Strategy (→ Chapter 2.4.1). At the time the CIP Strategy was adopted, critical infrastructure protection was also anchored in the updating (2008/2009) of the "Internal Security Programme" at the Standing Conference of State Interior Ministers and Senators (IMK 2009). This programme also considers intensifying cooperation between all state levels to be a necessity. Regular informal meetings have been taking place between the federal and state interior ministries since 2012. These meetings have proven their worth as a platform for exchanging views on cross-departmental issues of critical infrastructure protection and will be more closely linked to the formal committee structure of the interior ministries in future.

When it comes to critical infrastructure protection, cooperative partnership between state authorities and predominantly private sector operators is highly valued. In terms of the institutional structure, this can be seen in UP KRITIS – a platform for public and private sector cooperation between operators of critical infrastructure systems, their associations and the responsible state bodies (→ Chapter 2.4.2; UP KRITIS 2014a). On the one hand, the collaboration in UP KRITIS is expressed through a structured sharing of information about cyber security incidents, anomalies and the current level of IT threat (operational and tactical cooperation). On the other hand, relevant issues specific to certain industries are investigated in working groups organised both by industry and by topic (strategic and conceptual cooperation).

When it comes to implementing the *IT Security Law*, UP KRITIS acts as an interface between state bodies and the operators of critical infrastructures (BSI 2017a, → Infobox 16). UP KRITIS fulfills this role by developing the legal regulations used to identify critical infrastructures as defined by law. The UP KRITIS industry working groups were the first port of call when the expertise of the authorities and operators needed to be brought together in "core teams", tasked with tailoring the parameters of the regulatory framework so that it could be applied to specific industries. In addition, the UP KRITIS industry working groups have proven to be an ideal environment in which to develop "industry-specific security standards". With their help, it has been possible to put the stipulations of the *IT Security Law* into concrete terms for specific users in accordance with "the latest state of technology" (→ Chapter 2.2.2).

Collaboration between civil protection actors and the operators of critical infrastructures is decisive – in terms both of minimising risk and of crisis management. As such, the process of "integrated risk management" (BBK 2018a) is used to supplement the individual perspectives of each of the actors with the aim of creating a more holistic view. The focus is on building up interfaces and on sharing information, expertise, and results (→ Chapter 2.4.3). The procedure, which has now been tested multiple times in terms of its practical suitability, has recently been formalised in a DIN specification (DIN SPEC 91390:2019-12). The CIRMin research project (Critical Infrastructure – Resilience as a Minimum Supply Concept) has contributed to the development of integrated risk management (→ Infobox 17).

The Interstate and Interministerial Crisis Management Exercise (LÜKEX) focuses on the interplay between crisis management undertaken by operators and by state authorities (→ Chapter 2.4.4). Extraordinary crisis scenarios are modelled to put representatives from the state authorities and operators of critical infrastructures in extremely challenging situations that call for close and sustained interaction. The aim is to develop the skills of employees, to deepen the channels of communication with other parties participating in the exercise, and to work together to rehearse and improve the implementation of crisis management procedures. These exercises are systematically evaluated and documented (cf. BBK 2019b).

One scenario that has received a lot of attention from several actors in recent years is the "large-scale, prolonged power outage" (→ Chapter 2.4.5). In Germany, there is no one body with responsibility for emergency planning for power outages. Instead, a number of state actors working at the federal, regional and community levels and critical infrastructure operators each implement measures within their own fields of responsibility. The "Emergency Power Framework Concept" (Rahmenkonzept Notstrom) has been created to take a bird's eye view of this mishmash of measures, to record the state of knowledge on an ongoing basis, to develop tools, and to identify gaps in planning and information when it comes to emergency planning for power outages.

Its components include recommendations for establishing an emergency power supply (BBK 2015a, → Infobox 18) and fuel supply in the event of a power outage (BBK 2017, → Infobox 19), the development of emergency power capacities (THW 2014, → Infobox 20), and providing information to the general public (BBK 2019c, → Infobox 21).

Critical infrastructure protection as a sectoral task (→ Chapter 2.5)

When it comes to critical infrastructure protection, much importance is ascribed to accommodating connections and interdependencies between sectors. The fact that many approaches and activities within this field have a sectoral focus (→ Infobox 2) does not stand in contradiction to this. Rather, there is a need to substantiate overarching approaches for different sectoral contexts and to address fundamental issues in a sector-specific manner. For example, in many cases methods have been tailored for use within a sector, industry or even a specific type of facility, and sectoral networks related to critical infrastructure protection have also become established outside of UP KRITIS.

In 2006 and following a number of fatal incidents, including the fire at the Duchess Anna Amalia Library (2004) and the flooding of the River Elbe (2002), work began on the "Guidelines for the protection of cultural property" (SiLK), initiated by the German Conference of National Cultural Institutions (KNK). This web-based advice and evaluation tool covers topics concerning the protection of cultural property and is aimed at museums, libraries and archives as operators of important facilities within the CI sector *media and culture* (→ Chapter 2.5.1).

In order to sensitise and support operators and authorities working in the *water* sector, the BBK has published two recommendations on the security of the potable water supply (→ Chapter 2.5.2). The first part supports bodies responsible for the water supply in communities in investigating and assessing risks, particularly in conjunction with extraordinary threat levels (BBK 2019d). The second part describes the steps required to develop emergency planning (BBK 2019e).

The circulars issued by the Federal Financial Supervisory Authority (BaFin) play a central role in shaping risk management in the *finance and insurance* sector (→ Chapter 2.5.3). They define the minimum requirements for risk management (BaFin 2017) in the banking and financial services sector, and specify aspects of IT security for operators of critical infrastructures in the banking, insurance and capital management supervisory sectors (BaFin 2018a; BaFin 2019a; BaFin 2019b; → Chapter 2.5.3).

For hospitals, which constitute critical infrastructures within the *health* sector, methodological principles on risk and crisis management have been provided in various publications and tailored to the specific needs of hospitals. With the help of experts and partners, a guide for risk management in hospitals (BBK 2008) has been published.

The "IT Risk Analysis for Hospitals" (BSI 2013a) addressed IT security issues facing hospitals. The handbook on incident notification and response planning in hospitals, released in 2020, details planning measures that can be applied to maintain the capacity and functioning of hospitals in damaging situations (→ Chapter 2.5.4).

The BMVI Network of Experts brings together the expertise and know-how of seven departmental research institutes and specialist authorities in the business division of the Federal Ministry of Transport and Digital Infrastructure (BMVI) and also addresses questions concerning critical infrastructure protection in the *transport and traffic* sector. The current and expected future effects of climate-related extreme events on different modes of transport are being investigated in various thematic areas, with options for adaptation currently being developed (→ Chapter 2.5.5).

Cross-border cooperation in the field of critical infrastructure protection (→ Chapter 2.6)

The need for cross-border cooperation within Europe is reflected in three of the four fundamental freedoms of the European internal market, to which signatories are bound by treaty: the freedom to provide services, the free movement of goods, and the free movement of capital and payments as these form the constitutional basis of the European Union. In order to safeguard the ability of trans-European transport, energy, and telecommunication networks to function as part of the internal market, all member states must have a joint understanding of infrastructure security. In response to the terrorist attacks that took place in September 2001 on the one hand, and the challenges posed by digitalisation on the other, the European Commission has developed cross-sector initiatives to protect European and national critical infrastructures and, with the "EPCIP Directive" (RL 2008/114/EC) and the "NIS Directive" (RL 2016/11487/EU) in particular, has also influenced national legislation (→ Chapter 2.6.1).

Bilateral collaboration is also of great importance – it often occurs as part of reciprocal contracts, agreements or policy statements and put into practice by means of work programmes. The scope and intensity of cooperation varies and, depending on the agreement, ranges from a sharing of information and experience, to particular projects, to training and education programmes lasting several years. The "D-A-CH format" cooperation, which dates back to 2008, sees representatives from Germany, Austria, and Switzerland discuss programme-related considerations, methodological approaches and tangible measures, as well as differences and similarities in their respective approaches to critical infrastructure protection (→ Chapter 2.6.2).

Finally, cooperation within international organisations is also a key component when it comes to strengthening critical infrastructure protection at a national level (→ Chapter 2.6.3). Germany is a member of international organisations, including the North Atlantic Treaty Organization (NATO) and the Organisation for Economic Cooperation and Development (OECD), and also participates in the further development of critical infrastructure protection within these frameworks.

1

Chapter

Source: domin_domin / E+ / Getty Images

From the origins of critical infrastructure protection to a national strategy

This publication focuses on the activities that have been undertaken to implement the "National Strategy for Critical Infrastructure Protection" – or CIP Strategy (BMI 2009). When the strategy was adopted, the first steps regarding critical infrastructure protection had already been in place in Germany for over ten years. Prior to this, there had been discussions about the strategic focus and central concepts of critical infrastructure protection. Institutional frameworks from this policy area date from this period (→ Chapter 1.1). The CIP Strategy is based on this preliminary work and relates to it in a host of ways – for instance, in the way it continues existing forms of cooperation, provides a joint framework for processes that were previously separate, and replaces previously formulated strategic principles (→ Chapter 1.2). The following remarks draw attention to how critical infrastructure protection has developed over time and form the background for the information provided in → Chapter 2.

1.1 The origins of critical infrastructure protection in Germany

The beginnings of critical infrastructure protection as an independent topic are often associated with the so-called millennium issue ("Y2K") – the IT challenges posed by the transition from the 20th to the 21st century – or with the changing political and security situation following the terrorist attacks on September 11th. These were, of course, also milestones for critical infrastructure protection in Germany; however, the first signs of a systematic approach appeared in the late 1990s. This was when a final report by an expert commission in the USA was published, which prompted action on the international level at this time. The report, entitled "Critical Foundations", not only provided the impetus for grappling with the topic that has come to be known as "critical infrastructure protection"; the term itself also dates back to the work conducted by the expert commission (the President's Commission on Critical Infrastructure Protection) (PCCIP 1997).

In 1997, the Federal Ministry of the Interior (BMI) set up an interdepartmental working group on critical infrastructure protection. This was not just the first organisational structure established for the topic but, with its acronym "AG KRITIS", also marked the introduction of the German acronym "KRITIS". This acronym stands for "Kritische Infrastruktur(en)" and has been in use ever since in Germany. The English version of the acronym is CI, standing for critical infrastructure.

AG KRITIS was tasked with highlighting threat scenarios, identifying weaknesses in infrastructure that could be attacked through IT systems, and developing opportunities to avoid or reduce potential damage. Back then, "critical infrastructures" were defined as organisations and institutions that are vital for communities and whose failure or impairment would lead to long-term supply bottlenecks for large sections of the population or other dramatic consequences. AG KRITIS focused on seven sectors (→ Infobox 2). The tasks of the working group concluded with the publication of its final report in 2000. Its organisational successor had, however, been founded as early as 1998, when the first department dedicated to critical infrastructure protection at the federal level was created within the Federal Office for Information Security (BSI).

In response to the September 11th 2001 terrorist attacks, and following security meetings between the Federal Minister of the Interior and operators of critical infrastructures, an interdepartmental project group KRITIS (PG KRITIS) was established within the BMI in 2002. In addition to common risk assessments and a shared understanding of protection measures, the PG KRITIS group also agreed upon a definition of the term "critical infrastructures" and their classification into eight sectors, based upon the preliminary work that had been conducted by AG KRITIS (→ Infobox 2). Critical infrastructure protection may have been part of the federal government's overall anti-terrorism strategy at the time, but the activities still covered a wide range of threats. In terms of content, critical infrastructure protection addressed questions concerning so-called "physical protection" and IT security, i.e. protection against threats that arise specifically from the increased use of networked information technology in critical infrastructures. As a result, in 2001/2002, the BSI commissioned studies to provide an overview of the (then seven) CI sectors, to identify critical processes and to highlight their IT dependencies and vulnerabilities. As a result, the need for action concerning IT threats remained low at the time. In contrast, a high potential threat was predicted for physical threats.

Also in 2002, the "New Strategy for the Protection of the German Population" (BBK 2010), adopted by the Standing Conference of State Interior Ministers and Senators (IMK), took up the topic of critical infrastructure protection and placed it within the context of civil protection, an area of policy which was being restructured at the time. At the same time, a CI project group was set up in the Academy for Crisis Management, Emergency Planning and Civil Protection (AKNZ). Work then began on the study entitled "Risks for Germany" (BBK 2005), which took a detailed look at the importance of critical infrastructure protection for civil protection. Following the creation of the Federal Office of Civil Protection and Disaster Assistance (BBK) in 2004, the project group was moved to the "Centre of Critical Infrastructure Protection" within the BBK and with it, a second organisational unit focusing on critical infrastructure protection in addition to the BSI was created within a federal ministry. According to the 2003 explanatory memorandum on the *Act on the Establishment of the BBK,* the BBK is tasked with "planning precautions for the protection of the population and critical infrastructures ... insofar as this does not concern issues relating to the IT dependency of critical infrastructures", which fall under the responsibility of the BSI (cf. BT-Drs. 15/2286). From this point on, the two focal points – physical protection and IT security – were also reflected institutionally in the work of two authorities with different tasks; at the same time, this intensive cooperation between the BBK and BSI has shaped the development of critical infrastructure protection policy.

Recommendations for the cross-sector, physical protection of critical infrastructures were first published in 2005 in the so-called "Baseline Protection Concept" (BMI 2005a; → Infobox 1). In addition to a procedure for analysing potential threats, the Baseline Protection Concept features recommendations for structural, organisational, personnel-related and technical protective measures. The first edition of the "Protecting Critical Infrastructures – Risk and Crisis Management" guide (BMI 2007b, with the latest version, BMI 2011a, published two years later; → Chapter 2.1.1). This guide, which is intended for companies and authorities, presents methodological principles for establishing and developing risk and crisis management structures and provides relevant examples and checklists. The "National Plan for Information Infrastructure Protection" (NPSI, BMI 2005b), which was published in 2005 by the BMI, focused on information infrastructures. The NPSI was operationalised for operators of critical infrastructures and federal ministries with a "CIP Implementation Plan" (BMI 2007a) and the "Federal Implementation Plan" (latest version: BMI 2017). The CIP Implementation Plan marked the official start of the institutionalisation of the current UP KRITIS (UP KRITIS 2014a; → Chapter 2.4.2), a partnership between state authorities, operators and professional associations with the aim of improving critical infrastructure protection across industries and sectors.

Based on a decision by the IMK's working group (known as AK V) in 2007, an inter-state working group was set up under the auspices of the federal government, to draw up recommendations for cooperation between the federal and regional governments concerning critical infrastructure protection. The presentation of the report in autumn 2010 was accompanied by the working group's assessment that critical infrastructure protection is an ongoing task that requires coordinated action beyond the scope of the working group itself. Thus, the foundations were laid for strengthening the protection of critical infrastructures, including across administrative levels (→ Chapter 2.4.1).

The issue of critical infrastructure protection had significantly picked up speed within the European Union by 2004 at the latest (→ Chapter 2.6.1). The publication of the European Commission's Communication on critical infrastructure protection in the fight against terrorism (KOM 2004) and the "European Programme for Critical Infrastructure Protection" (EPCIP, KOM 2006) had a lasting impact not only on policy and strategy, but also on the legal frameworks for critical infrastructure protection in Germany and in other member states.

Infobox 1: The Baseline Protection Concept

During 2004, the BMI prompted the development of a concept for the "physical protection" of facilities and plants that could be used across different industries. The guide entitled "Protection of Critical Infrastructures – Baseline Protection Concept. Recommendations for Companies" (BMI 2005a), or the "Baseline Protection Concept" for short, was the result. It comprises the traditional measures that had in part already been described in legal provisions, such as the *Hazardous Incident Ordinance* or the *German Stock Corporation Act,* but these have been made more accessible to the broader public as a result of the guide. Even though the Baseline Protection Concept is based on an All-Hazards Approach, there is a specific focus on terrorist threats and crime – which comes as no surprise given it was published soon after the March 2004 terrorist attacks in Madrid.

In the guide, "baseline protection" is understood as "minimum protection" (BMI 2005a, p. 18) and it adopts a generalised approach that has as broad an application as possible. Specific steps for a structured analysis and planning process are provided as examples, risk factors are explained and types of threats described; however, the list of questions and sample checklist are left somewhat abstract. It is essential that the information is supplemented with special protection concepts specific to different sectors and industries, and adapted to suit the particular needs of different companies. A step-by-step approach for this is outlined in the Baseline Protection Concept: while the role of the state decreases from the first to the third steps to make way for the companies in question, the amount of information required also shifts from publicly accessible sources to internal company data.

Figure 1: The Baseline Protection Concept (BMI 2005a) relates to the *Hazardous Incident Ordinance* (source: Johner Images/Getty Images).

Even though the Baseline Protection Concept was intended to be a "mandatory programme" to be implemented by all companies, it was met with great interest at both the national and international level. This acceptance is surely because the concept was developed by a working group including operators themselves; in other words, the experts involved were also the target audience for the Baseline Protection Concept. This constellation of actors went on to prove its worth time and again during the development of methodological principles for critical infrastructure protection (→ Chapter 2.1).

1.2 A strategic framework: the National Strategy for Critical Infrastructure Protection (CIP Strategy)

As work began on critical infrastructure protection in Germany in the late 1990s, a wide range of activities were undertaken: both general recommendations and special handouts were compiled, studies were conducted and organisational structures established (→ Chapter 1.1). However, there was no coherent approach that followed a single strategic objective. The NPSI (BMI 2005b) and its "CIP Implementation Plan" (BMI 2007a) in particular were already leading the way here: strategic objectives were formulated for prevention, response and the sustainability of measures for maintaining critical business processes. Furthermore, a roadmap announced the setting up of working groups for emergency response and crisis exercises, crisis reactions and crisis management, maintaining critical infrastructure services, as well as national and international cooperation. In accordance with the NPSI, the CIP Implementation Plan focused on the protection of *information* infrastructures and predominantly addresses private operators of critical infrastructures.

The first considerations of a holistic strategy for critical infrastructure protection began to develop from 2007 onwards. Key strategic decisions were made in a benchmark paper, and these were also included in the strategy that was adopted in 2009. The discussions concerning the key points, a guiding policy concept, and the first preliminary drafts of a strategy were initially held between the responsible departments in the former BMI and the two division authorities, the BBK and BSI. By mid-2008, the draft of the strategy was ready to be put to an initial interministerial consultation and then, at the beginning of 2009, was passed following a second interministerial consultation. The regional governments and industry stakeholders also shared their views on the draft, before the federal cabinet approved the CIP Strategy (BMI 2009) in June 2009.

By this time, critical infrastructure protection measures had been in place for over a decade (→ Chapter 1.1). Thus, as is described in the guiding policy concept, the strategy summarises "the aims and objectives and its political-strategic approach that is already applied in practice […] and is the starting point for consolidating the results achieved so far and for further developing them in view of novel challenges" (BMI 2009, p. 2). Regarding what had been achieved thus far, a chapter entitled "Progress made so far, and present status" (BMI 2009, p. 3f.) cites preventative IT security measures, such as the IT Baseline Protection and the NPSI, including its CIP Implementation Plan, which had established collaboration between the authorities and the operators of critical infrastructure. This cooperation had already been noted in the "Baseline Protection Concept" (BMI 2005a) and in the guide on risk and crisis management for companies and government authorities (BMI 2007b, → Chapter 2.1.1) as well as in the involvement of operators in the "Interstate and Interministerial Crisis Management Exercise (LÜKEX)" (→ Chapter 2.4.4). In addition, the launch of the programme "Research for Civil Security" (BMBF 2007, → Chapter 2.3.3) was also listed as an achievement here. The CIP Strategy identifies future challenges for critical infrastructure protection as an aspect of internal security in the context of a growing societal dependence on increasingly interlinked infrastructure systems and with regard to a new level of terrorist threats and natural hazards. Thus, it is necessary to address a wide range of critical infrastructures and a broad spectrum of threats (cf. BMI 2009, p. 3f.).

It follows that one of the core elements of the CIP Strategy is its orientation around the so-called "All-Hazards Approach" (cf. Table 1). According to the strategy, "Critical infrastructure may be exposed to various threats which must be included both in risk and threat analyses and in the selection of options for action" (BMI 2009, p. 7). In accordance with this, hazard-specific activities form individual components. The CIP Strategy thus provides a common framework for activities designed to safeguard the IT security of critical infrastructures and so-called "physical protection".

Natural events	Technical failure / Human error	Terrorism, crime, war
Extreme weather events inter alia, storms, heavy precipitation, drops in temperature, floods, heat waves, droughts	System failure inter alia, insufficient or excessive complexity of planning, defective hardware and/or software bugs	Terrorism
Forest and heathland fires	Negligence	Sabotage
Seismic events	Accidents and emergencies	Other forms of crime
Epidemics and pandemics in humans, animals and plants	Failures in organisation inter alia, shortcomings in risk and crisis management, inadequate coordination and cooperation	Civil wars and wars
Cosmic events inter alia, solar storms, meteorites and comets		

Table 1: Overview of the CIP Strategy's "All-Hazards Approach" (source: BMI 2009, p. 7, translated by: BMI).

A further central element of the strategy is the continuation of an approach already outlined in the CIP Implementation Plan: the focus of critical infrastructure protection across all phases of risk and crisis management (cf. Figure 2). For "prevention", risks should be identified in advance and serious disruptions and outages avoided wherever possible or reduced to a minimum; for "response", the consequences of disruptions and outages should be kept to a minimum by means of emergency management, redundancies, and self-help capacity (cf. BMI 2009, p. 10). Findings regarding hazards need to be updated in ongoing analyses. The implementation status is to be reviewed and updated in evaluation processes. The measures taken should also be practised on a regular basis. Lessons learnt from previous incidents and from the sharing of experiences between actors domestically and abroad are viewed as sub-aspects of the "sustainability" of critical infrastructure protection (cf. BMI 2009, p. 10-11).

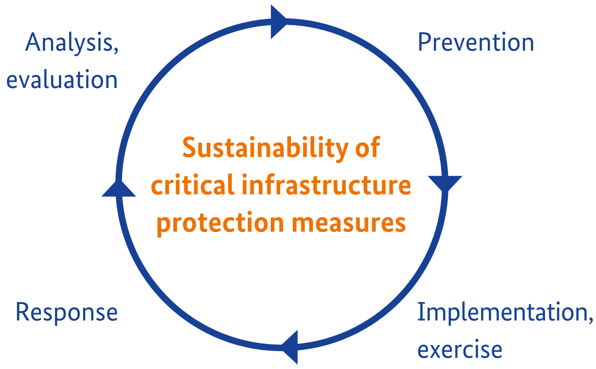


Figure 2: Schematic diagram on "Risk management circle for critical infrastructures" (source: BMI 2009, p. 11, translated by: BMI).

The strategy may be predominantly directed at the federal government, but it also addresses many other actors: state authorities at all levels, as well as operators of critical infrastructures and their associations, science and research and, not least, the general population. The various actors each assume different roles and differ in terms of the intention, content and intensity of their involvement with critical infrastructure protection: from "guarantors" (the state) and "providers" (operators), to "developers" (science and research) and "essential users".

Special importance is attached to cooperation between the state and industry, as these two entities are responsible for the availability of key infrastructures. The "cooperative approach" is at the heart of this: i.e. cooperation that is characterised by common interests and common goals, and that complements the classic relationship of superiority/subordination in the sovereign state in favour of collaboration in the spirit of partnership. According to the CIP Strategy guiding policy concept, the state regulates critical infrastructure protection, "either – primarily – as a moderator or – if required – by rule-making" (BMI 2009, p. 2); in other words, priority is given to voluntary self-commitment over statutory regulation. For companies, proportionality – i.e. the necessity, suitability and appropriateness of the means – is a guiding principle when it comes to critical infrastructure protection (BMI 2009, p. 10).

The strategy only gives a rough idea of how cooperation between state authorities on the one hand and private actors on the other can be structured and implemented. The milestones provided include the setting of protection objectives, the analysis and evaluation of threats, and the agreement on protection measures and their implementation, as well as a continuous risk communication process (cf. BMI 2009, p. 14). This approach to cooperation between the state and private sector can be applied at all administrative levels (federal, regional and community) and, although the strategy as a federal strategy is predominantly aimed at actors working at the federal level, its cross-level perspective is also evident.

When viewed as a whole, the CIP Strategy is more of a guide than a fixed set of rules for a structured approach to critical infrastructure protection in Germany. As such, the individual work packages described in the strategy are not given in detail; rather they are to be expanded upon as the strategy is implemented. → Chapter 2 provides an insight into the activities that have been undertaken on this basis over the past ten years.

Infobox 2: Sectors and branches of critical infrastructure over time

A number of sectors have been classified over the years in order to substantiate the field of critical infrastructure protection. These classifications are the result of discussions about the focus of critical infrastructure protection and also serve to reflect how the field of policy has developed over time. The first version came from the interdepartmental AG KRITIS working group, which was set up in 1997, and which presented its final report in 2000 (→ Chapter 1.1). This classification comprised seven sectors (cf. Table 2). Even though the name of the *healthcare* sector does not make it immediately obvious, the supply of drinking water and food was also included. This first sector classification by AG KRITIS was used in the BSI's 2003 annual report, for example (cf. BSI 2004).

PG KRITIS, formed in 2002, stipulated a total of eight sectors (cf. Table 2). One sector entitled *supply of vital goods and services* combined the supply of water, food, and healthcare services, as well as crisis management. PG KRITIS introduced the *media* and *cultural property* sectors, which are still present in a similar form in the most recent sector classification. By contrast, the approach taken by PG KRITIS to also include large research facilities and the *hazardous substances* sector in the classification was not continued. The latter differs from the other sectors in that it does not represent a "service sector" worth protecting due to its importance to society. The threat from hazardous substances relates to their release and not to the failure of a service. In this respect, the inclusion of this sector suggests a different, broader understanding of what constitutes *critical* infrastructure and the aims of critical infrastructure protection. The PG KRITIS sector classification was published in the NPSI (BMI 2005b) and later in the first edition of the guide on risk and crisis management for companies and government authorities (BMI 2007b).

Discussions regarding a new sector classification scheme had not yet been concluded by the time the CIP Strategy (BMI 2009) was passed in 2009 (→ Chapter 1.2). For this reason, the CIP Strategy contains an overview of "technical basic infrastructures" and "socio-economic services infrastructures” (cf. BMI 2009, p. 5), rather than a specific sector classification. It wasn’t until 2011 that a classification into the current nine CI sectors was agreed upon between the federal departments and regional governments (cf. Table 2) and published, for example in the revised second edition of the guide on risk and crisis management (BMI 2011a). The most obvious change, aside from the omission of the *hazardous substances* sector, was the division of the previous *supply of vital goods and services* sector into three separate ones, namely *food, health* and *water* (BBK/BSI 2011). This sector classification, which is still valid to this day, has been further broken down at the federal level into 29 individual branches (cf. Table 3). When these are added to the mix, it becomes apparent that some of the terms used to describe sectors in previous versions are now used at the branch level, for instance the *judiciary* or *emergency and rescue services.*

AG KRITIS sector classification (BSI 2004, p. 67)	PG KRITIS sector classification (BMI 2005b, p. 21)	Current sector classification by the federal and regional governments (BMI 2011a, p. 8; BBK/BSI 2011)
Energy	**Energy** (electricity, oil, gas)	**Energy**
Telecommunications and information technology	**Information technology and telecommunication**	**Information technology and telecommunication**
The transport system	**Transport**	**Transport and traffic**
Healthcare (incl. food and drinking water supplies)	**Supply of vital goods and services** (public health service, emergency and rescue services, civil protection, food and drinking water supply, waste disposal)	**Health**
		Water
		Food
Emergency services		*
Financial and insurance systems	**The financial, monetary and insurance system**	**Finance and insurance**
Public agencies and public administration	**Public authorities, the administration, the judiciary** (incl. police, customs and federal armed forces)	**State and administration**
	Other (the media, large research institutions, architectural buildings of outstanding and symbolic value, cultural heritage)	**Media and culture**
	Hazardous substances (chemical and biological agents, transport of hazardous material, arms industry)	

*Note: Emergency services is a branch within the *state and administration* sector

Table 2: How the classification of critical infrastructure sectors has developed over time and the latest version (compiled by: BBK).

Sector classification (federal and regional level) (BBK/BSI 2011)	Branch classification (federal level) (BBK/BSI 2011)	Critical services (current state of discussion) (BBK 2019a, p. 38)
Energy	Electricity, gas, petroleum, district heating	Electricity supply, gas supply, fuel and heating oil supply, district heating supply
Food	Food industry, food retail trade	Food supply
Finance and insurance	Banks, stock exchanges, financial service providers, insurance	Monetary transactions, cash supply, bank lending, trading in securities and derivatives, insurance services
Health	Medical care, medicines and medical products, laboratories	Medical care, supply of medicines (including vaccinations and protective materials according to radiation protection law), supply of medical products, laboratory diagnostics
Information technology and telecommunications	Telecommunications, information technology	Cable-based and wireless (also space-based) language and data transmission, data storage and data processing
Media and culture	Broadcasting (television and radio), printed and electronic media, archives, museums and libraries, cultural monuments and historic sites	Warnings and alarms, supply of information, establishing a public sphere, storing cultural objects and documents that provide a common identity, conveying a cultural identity, archiving and storage of micro-filmed documents from German history in accordance with the Hague Convention for the Protection of Cultural Property
State and administration	Governance and administration (executive), parliament (legislative), judiciary and judicial institutions, emergency and rescue services	Implementation of law as part of the administration of regulations and services, (police and non-police) emergency prevention, defence, legislation, control of the government, dispensation of justice and its execution
Transport and traffic	Air transport, maritime transport, inland waterway transport, road transport, logistics, rail transport, logistics	Services for transporting people, services for transporting goods, satellite navigation systems and satellite-based positioning, navigation, time and meteorological services
Water	Public water supply, public waste water disposal	Drinking water supply, waste water disposal

Table 3: Currently applicable classification of critical infrastructure sectors agreed between the federal and regional governments, branch classification from a federal perspective, and the latest state of discussion about critical services (compiled by: BBK).

A little later, the concept of a "critical service" became significant within the context of critical infrastructures. The term refers to a "service that is provided by operators of critical infrastructures to supply the general public and the failure or limitation of which would lead to considerable bottlenecks in supply, to threats to public safety or to similar consequences" (BBK 2019f, p. 34). Critical infrastructures are of special importance to the provision of critical services within the sectors and branches. As such, the term critical service does not add anything novel to the discussion, but it does serve to complete the system of terms with a central aspect and also documents a certain change of focus – from protecting the infrastructure to maintaining a service. The notion of critical services has gained in importance in recent years, not least as a result of the *IT Security Law* and the *BSI Critical Infrastructure Ordinance,* which was issued for its implementation (→ Chapter 2.2.1 and Infobox 16). The list of critical services in Table 3 reflects the current state of discussion (BBK 2019a; → Chapter 2.1.2).

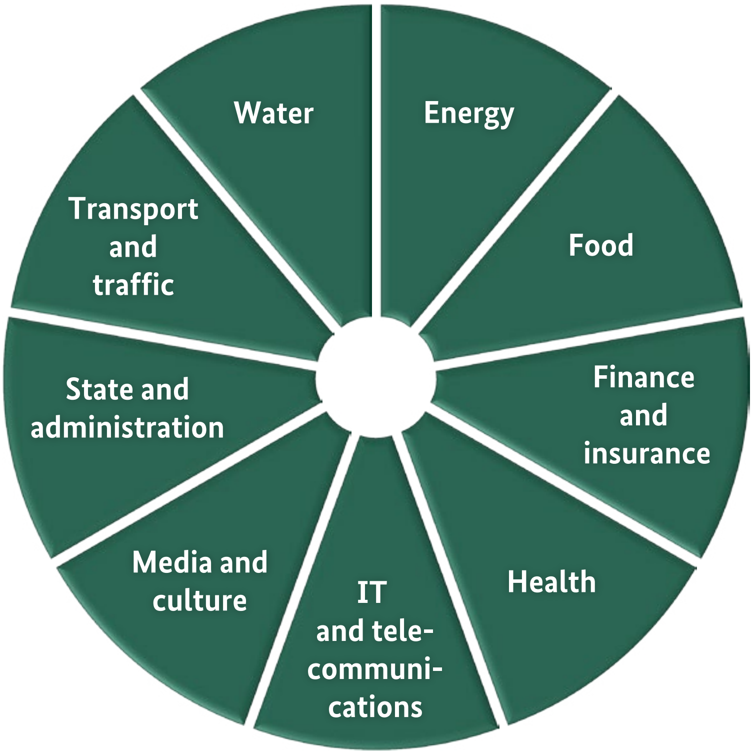


Figure 3: The sectors are often displayed as a pie chart (here in alphabetical order; source: BBK/ BSI 2011, translated by: BBK).

2

Chapter

Source: Natalia Klenova / EyeEm / Getty Images

The factors affecting critical infrastructure protection over the past ten years

The anniversary of the CIP Strategy (BMI 2009) presents an occasion to look back on the many steps that have been taken in the field of critical infrastructure protection over the past ten years. What follows does not constitute a full review; rather, as the title suggests, it is a series of insights into various aspects that have shaped the field of policy over this period as well as how the issue has developed as a result.

These aspects also include shining more light on the strategy's prominently placed demand to achieve a universal approach to critical infrastructure protection and a perspective that goes above and beyond the individual actors concerned. Both of these are considered in detail in separate chapters, but are also expressed in the form of this publication: a number of different institutions, in particular the federal ministries from various departments, have been involved in the following insights. Their input includes their own specific viewpoint regarding critical infrastructure protection. We would like to give special thanks to the following groups for their willingness to participate in this publication and for providing contributions from their own work:

- the Federal Ministry of the Interior, Building and Community (BMI) and its division authorities: the Federal Office for Information Security (BSI), the Federal Agency for Technical Relief (THW), and the Federal Institute for Research on Building, Urban Affairs and Spatial Development (BBSR), which is part of the Federal Office for Building and Regional Planning (BBR),
- the Federal Ministry of Finance (BMF) and the Federal Financial Supervisory Authority (BaFin),
- the Federal Ministry of Education and Research (BMBF),
- the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU),
- the Federal Ministry of Transport and Digital Infrastructure (BMVI),
- the Federal Ministry of Economic Affairs and Energy (BMWi) and the Federal Network Agency (BNetzA),
- the Federal Office for Agriculture and Food (BLE),
- the Office of the National Focal Point for the Sendai Framework (NKS) at the BBK and
- the SiLK team at the German Conference of National Cultural Institutions (KNK).

The contributions that form the following chapter have been broken down by topic:

- The development and implementation of methodological principles (→ Chapter 2.1)
- Creating the operational framework (→ Chapter 2.2)
- Critical infrastructure protection as a cross-sectoral issue (→ Chapter 2.3)
- and as a task requiring cooperation between actors (→ Chapter 2.4),
- as a sectoral task (→ Chapter 2.5) and
- as a cross-border task (→ Chapter 2.6).

Many of the contributions are also closely linked to other topics: thus, for example, cooperation at the European level can help to establish the legal framework, and forms of cooperation between sectors can help to advance the development of methodological principles. As a result, the reports below include a wealth of cross-references. Readers can either follow the structure of the text or can use the references to gain an impression of what has played a part in shaping critical infrastructure protection over the past ten years.

2.1

Chapter

Source: Sean Gladwell / Moment / Getty Images

The development and implementation of methodological principles

Methodological principles are courses of action for specific groups and areas of application and thus perform various functions within the context of critical infrastructure protection. They substantiate a field of discourse, formulate the expectations placed on individual groups of actors, structure the cooperation between these actors, and create a link to established procedures. Some are incorporated in binding directives or formal instruments, while others serve purely as orientation. Methodological principles start to have an impact as early as the development phase: they encourage those involved to grapple more intensively with the topic in question and have often acted as the starting point for cooperation between actors.

Operators of critical infrastructures – whether companies or authorities – are responsible for ensuring the safe and reliable operation of their plants and facilities. As such, the guide for a facility-related risk and crisis management for operators of critical infrastructures from all branches is one of the central methodological principles for critical infrastructure protection (→ Chapter 2.1.1). The methodology presented in this guide is based on recognised standards, which have been tailored to critical infrastructure protection in close cooperation with relevant operators. In addition, a series of industry-specific guides, as well as procedures governing structured collaboration between operators and state authorities for risk and crisis management, have been drawn up (→ Chapter 2.5.2 and Chapter 2.5.4).

In order to ensure that operators of critical infrastructures are aware of their special responsibility and that state bodies can find points of contact within private operators, a methodology for identifying critical infrastructures has been developed and published as a guide (→ Chapter 2.1.2).

Whether or not a particular plant or facility is considered to be critical depends on the approach, so the methodology described here can be adapted to suit the respective context in which it is being applied. One application at the federal level is the identification of critical infrastructures within the terms of the *IT Security Act,* which is governed by the *BSI Critical Infrastructure Ordinance* (→ Infobox 16). The Hague Convention identifies a cultural property as something that especially reflects the identity of communities (→ Infobox 3).

The national risk analysis for civil protection investigates the impact that different risk events would be expected to have on the population and its basic needs (→ Chapter 2.1.3). The consequences of storms or pandemics are, for example, largely dependent on the degree to which they affect critical services. Once a scenario has been stipulated in the risk analysis, the next step is to investigate the impact on critical infrastructures so that effects can be viewed as a whole. The failure of critical infrastructures as an “indirect” consequence of an event thus occupies a key position in the methodology for risk analysis in civil protection.

With its spatial approach to risk management, spatial planning offers a cross-sector perspective on critical infrastructure protection. It can highlight where a focus on individual, industry-specific safety regulations falls short or would stand in the way of an integrated solution, for example due to the spatial proximity of different infrastructures. Suitable methodological principles need to be developed in order to be able to make best use of the opportunities presented by preventative risk management, for example in regional planning (→ Chapter 2.1.4).

2.1.1 Risk and crisis management for operators of critical infrastructures

Responsibility for ensuring the functionality of critical infrastructures lies with operators, whether these are private companies or public institutions. It is incumbent upon them to calculate the risks for their plants and facilities in a structured way and to use this risk analysis to implement precautionary measures (risk management) in order to avoid disruptions or outages to critical infrastructures wherever possible or to reduce the impact of these should they occur. At the same time, they are required to establish procedures so that crises can be handled in an effective and efficient way (crisis management): in case of an incident, procedures must be followed to reduce the negative effects of outages and to support a rapid return to normal operations. So, comprehensive risk and crisis management by the operators of critical infrastructures is fundamental to maintaining supply when it comes to critical services.

To support state and private operators of critical infrastructures in establishing risk and crisis management systems, the BMI collaborated with the BBK and BSI, as well as experts from the private sector, to publish a guide in 2007 entitled "Protecting Critical Infrastructures – Risk and Crisis Management. A guide for companies and government authorities", which was revised in 2011 (BMI 2011a). In five phases the guide describes the methodological principles underlying the establishment of a risk and crisis management system within facilities and sets out feasible ways to improve existing arrangements (cf. Figure 4).

The guide is based on internationally recognised procedures, such as DIN ISO 31000 "Risk Management – Guidelines", and lays out specific requirements for the risk and crisis management systems of critical infrastructures (→ Chapter 2.2.2).

The descriptions of the methodology provided in this guide can be applied by operators of critical infrastructures across all sectors and branches (→ Infobox 2). To be able to provide recommended courses of action specific to individual industries, a whole series of further guides was subsequently drawn up based on this methodology. These guides cover subjects including how to carry out risk analyses in drinking water supply (→ Chapter 2.5.2) or risk management in hospitals (→ Chapter 2.5.4), for example, and address industry-specific aspects that are not covered in the more general guide.

The risk and crisis management guide for companies and authorities is aimed at operators of critical infrastructures. However, when it comes to preparing for and dealing with an incident, cooperation between operators and the relevant state authorities is paramount. Thus, in an ideal situation, close links between a company and the authority's risk and crisis management systems will already have been established at an early stage (→ Chapter 2.4.3). The process for developing an integrated risk management system, which has this aim in mind, is also based on the method presented in Figure 4.

To make it easier to access the risk and crisis management system, employees from private companies and authorities can attend seminars and exercises at the BBK's Academy for Crisis Management, Emergency Planning and Civil Protection (AKNZ). The content covered in these sessions builds upon the risk and crisis management guide for companies and authorities.

2.1.2 Critical or not? Identification methodology

The federal and regional governments have agreed upon the classification of critical infrastructure sectors. At the federal level, these sectors have also been split up into branches (→ Infobox 2). However, it is still not possible to cite specific facilities or plants or to address their operators directly on this basis alone. This is a necessary step for enabling operators to be made aware of their special responsibilities for protecting the infrastructures they operate and to ensure that authorities know which operators

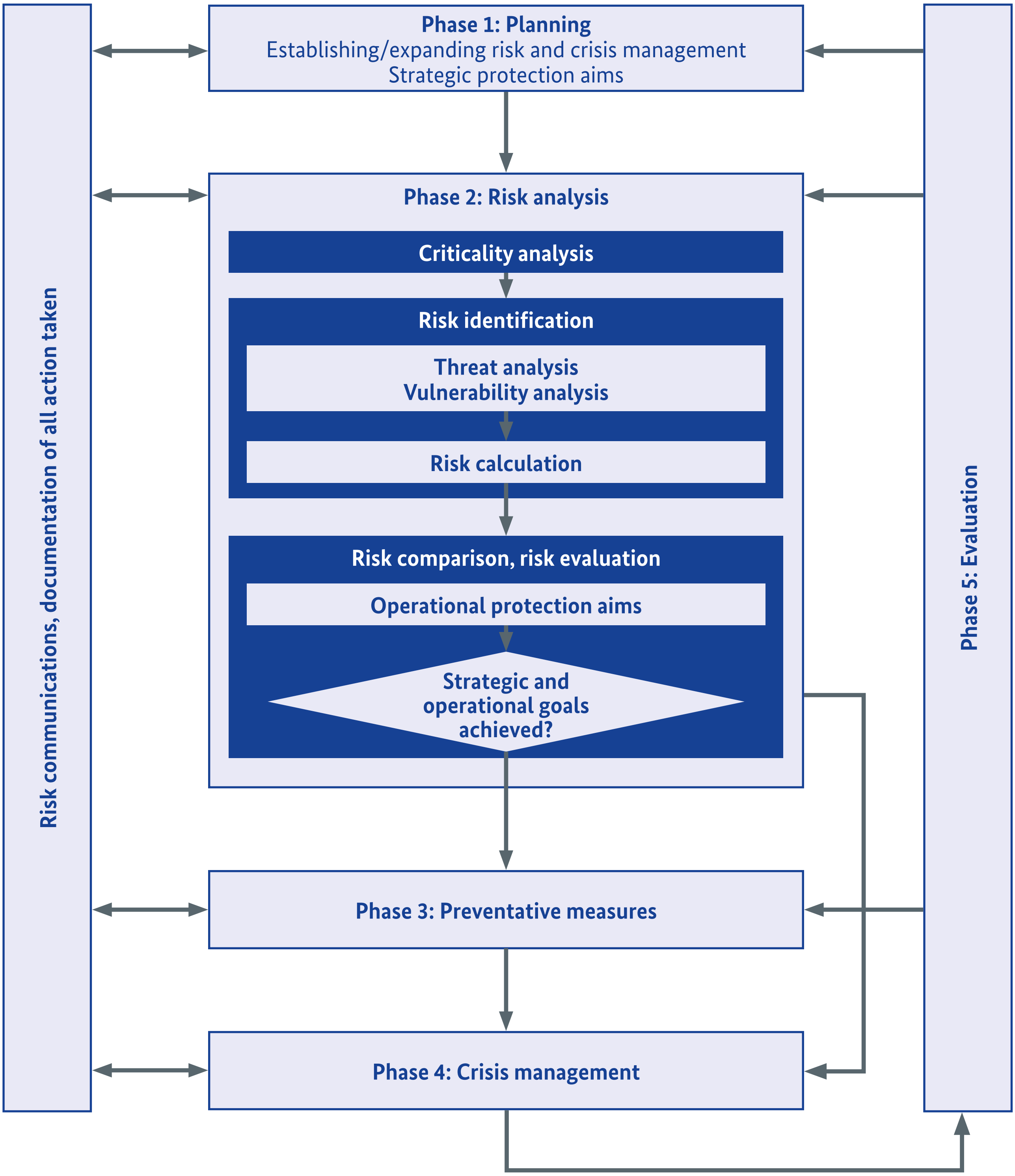
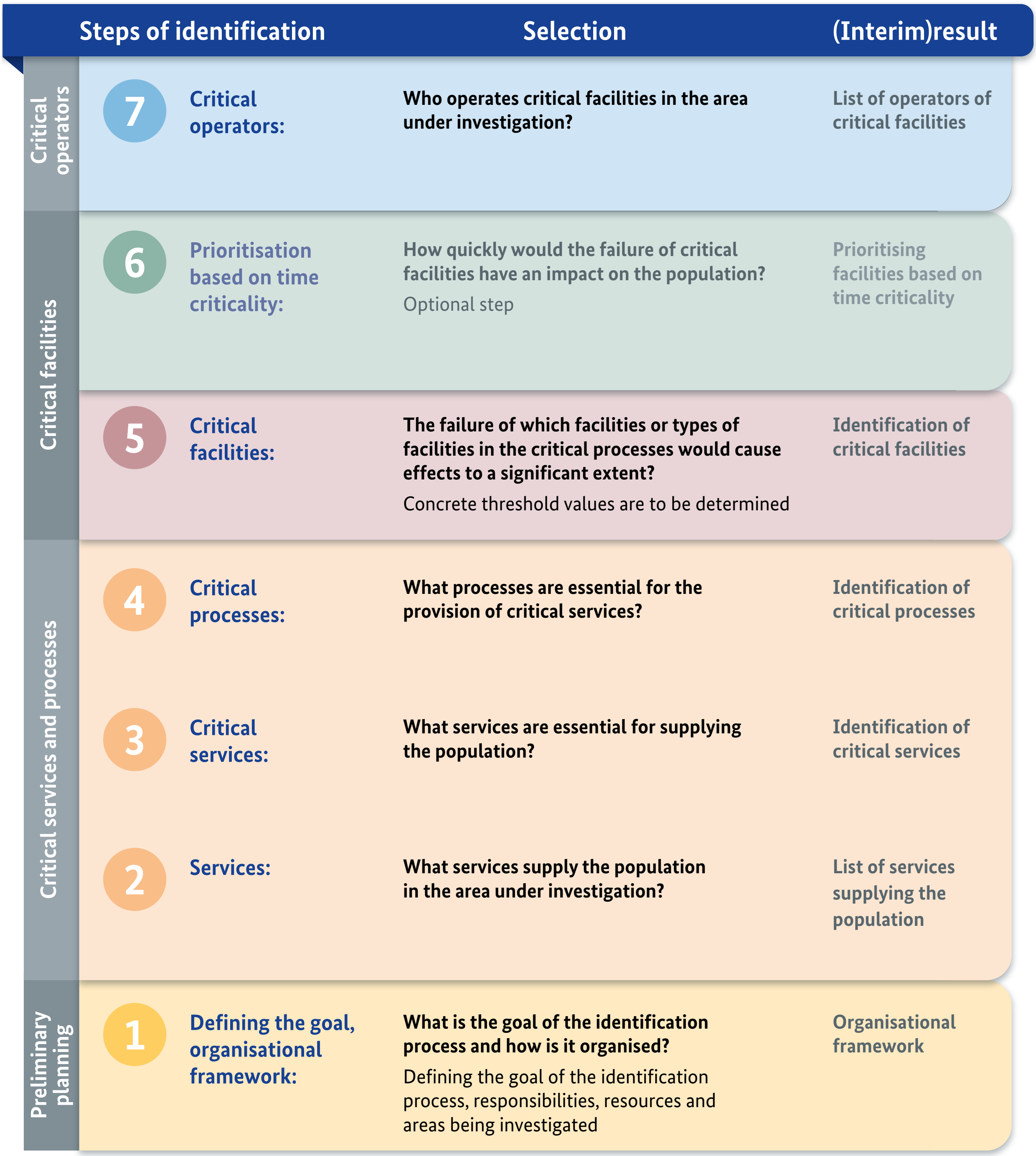

Phase 1: Planning
Establishing/expanding risk and crisis management
Strategic protection aims
Phase 2: Risk analysis
Criticality analysis
Risk identification
Threat analysis
Vulnerability analysis
Risk calculation
Risk comparison, risk evaluation
Operational protection aims
Strategic and operational goals achieved?
Phase 3: Preventative measures
Phase 4: Crisis management
Risk communications, documentation of all action taken
Phase 5: Evaluation

Figure 4: Diagram showing risk and crisis management (based on: BMI 2011a, p. 12, translated by: BBK).

they should coordinate with, for example as part of an integrated risk management system (→ Chapter 2.4.3).

Depending on the issue, identifying critical services, processes, plants/facilities or their operators is part of risk management, both in terms of civil protection and from the CI operator's point of view. The topic of identification is thus central to critical infrastructure protection.



		Steps of identification	Selection	(Interim)result
Critical operators	7	Critical operators:	Who operates critical facilities in the area under investigation?	List of operators of critical facilities
Critical facilities	6	Prioritisation based on time criticality:	How quickly would the failure of critical facilities have an impact on the population? Optional step	Prioritising facilities based on time criticality
	5	Critical facilities:	The failure of which facilities or types of facilities in the critical processes would cause effects to a significant extent? Concrete threshold values are to be determined	Identification of critical facilities
Critical services and processes	4	Critical processes:	What processes are essential for the provision of critical services?	Identification of critical processes
	3	Critical services:	What services are essential for supplying the population?	Identification of critical services
	2	Services:	What services supply the population in the area under investigation?	List of services supplying the population
Preliminary planning	1	Defining the goal, organisational framework:	What is the goal of the identification process and how is it organised? Defining the goal of the identification process, responsibilities, resources and areas being investigated	Organisational framework

Figure 5: An overview of the seven step identification process (source: BBK 2019a, p. 23, translated by: BBK).

To make the identification process easier, the guide entitled “Protecting Critical Infrastructures – A Seven Step Identification Process” (BBK 2019a) provides step-by-step information about the methodological approach. In this way, critical services, processes, facilities/plants and operators can be identified and incorporated into risk management across a range of different application contexts and levels. The BBK is currently supporting some users as they implement this method.

The federal departments have agreed not to keep a central register of all critical infrastructures and their operators. Security considerations make up one argument against such a register, as it would include extremely sensitive information. Whether a facility is classed as critical and whether its operator is considered to be an operator of critical infrastructure also depends on the level at which it is being viewed: for example, a facility not considered to be critical at the federal level could be of crucial importance for hazard control at a local level. As such, the question is not "critical – yes or no?", but rather "critical within this context – yes or no?".

The need to identify individual facilities or plants as critical and to name their specific operator is of particular importance within the context of legislation: in accordance with the principle of clarity, the addressees of a statutory provision must be clearly identifiable. Thus, in order to implement an EU directive (cf. Directive 2008/114/EC), an identification procedure was used to determine "critical *European* infrastructures" in the transport and energy sectors (→ Chapter 2.2.1 and Infobox 5). At the national level, the passing of the *IT Security Law* in 2015 made it necessary to stipulate and carry out an identification process. The *BSI Critical Infrastructure Ordinance* (→ Infobox 16) specifies which facilities are "critical within the context of the IT Security Law". The regulation is based on the same identification method described in the aforementioned guide – it is, therefore, a specific application of the method, but one that can be used in different contexts.

Infobox 3: A special case: identifying cultural property in the context of the Hague Convention

Many cultural properties especially reflect the identity of communities. In this case, one refers to a high "symbolic criticality" (BMI 2009, p. 5). The loss of this cultural property can disrupt a society and psychologically unbalance its members. Damage to cultural property can also occur as a result of war. Cultural properties face the risk of becoming damaged, destroyed or stolen in these situations precisely because of their symbolic criticality.

As a result, the Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict – or, in the context of this report, "the Hague Convention" – was negotiated by the United Nations Educational, Scientific and Cultural Organization (UNESCO). It was passed in 1954, is part of international humanitarian law and has since been ratified by 133 countries, including Germany (cf. *Law on the Convention of 14th May 1954 for the Protection of Cultural Property in the Event of Armed Conflict* from 11th April 1967). The cultural sovereignty of Germany's constituent regional states is enshrined in law (Art. 30 GG), and the federal government is responsible for implementing the convention as a special case relating to armed conflicts. This task is part of the BMI's remit and is administered on behalf of the federal government by the BBK and by the states. Implementing the Hague Convention is part of the "Civil Defence Concept" (BMI 2016b, → Chapter 2.3.2).

Because not all cultural property can be protected equally, the objects considered to be at particular risk within the context of the Hague Convention need to be identified. Here, "particular risk" refers to those cultural objects that are well-known and that many people feel an emotional connection with. It does not just concern "particularly high-value" monuments or works of art in the view of the public, but also refers to their symbolic value and significance for the populace. Around 10,000 objects had been listed by the 1980s, but there remain doubts about the topicality and manageability of the lists already compiled. The notion of symbolic criticality offers a novel perspective regarding the identification of endangered objects and offers criteria for evaluating their importance.

Figure 6: The "Blue Shield" is the international symbol for cultural property according to the Hague Convention (source: UNESCO).

2.1.3 Critical infrastructures as part of the national risk analysis for civil protection

Before we can assess how to deal with risks appropriately and draw up targeted plans for civil protection, it is vital to identify which threats are present, what consequences they could have and how prepared civil protection would be if such threats occurred.

These questions form the national risk analysis for civil protection. This risk analysis has been anchored in Section 18 of the *Federal Civil Protection and Disaster Assistance Act* (→ Chapter 2.2.1) since 2009 and is implemented by the federal government, working in collaboration with regional authorities. The BMI must report back to the German Bundestag each year on its implementation. The results of the analyses are published as parliamentary documents.

The following risk analyses have been carried out to date:

- Extreme flooding caused by meltwater from the central mountains (2012, BT-Drs. 17/12051)
- Pandemic caused by the Modi-SARS virus (2012, BT-Drs. 17/12051)
- Winter storm (2013, BT-Drs. 18/208)
- Storm surge (2014, BT-Drs. 18/3682)
- Release of radioactive substances from a nuclear power plant (2015, BT-Drs. 18/7209)
- Release of chemical substances (2016, BT-Drs. 18/10850)
- Review of existing risk analyses (2017, BT-Drs. 19/9520)
- Drought (2018, BT-Drs. 19/9521)
- 2019 and ongoing: Earthquake

The risk analyses are based on fictional scenarios representing a plausible sequence of events. The

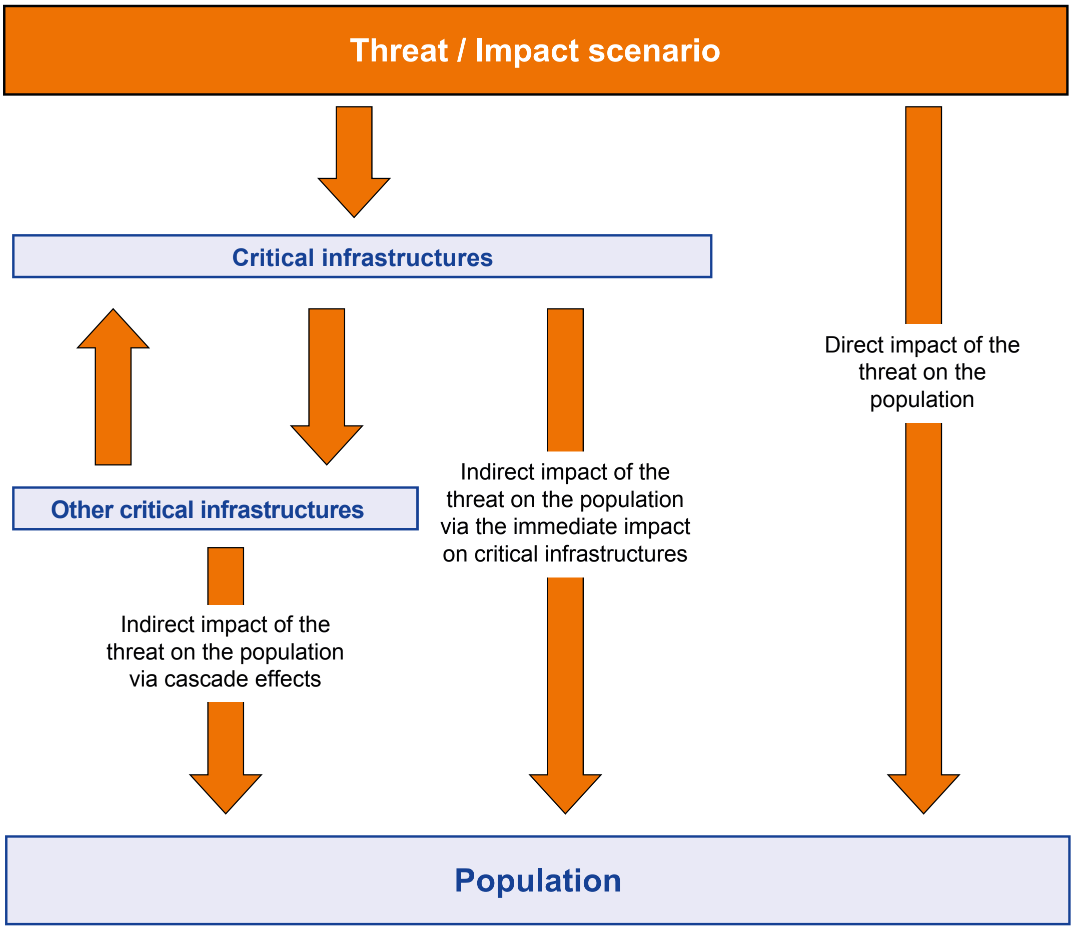

Threat / Impact scenario
Critical infrastructures
Other critical infrastructures
Indirect impact of the threat on the population via cascade effects
Indirect impact of the threat on the population via the immediate impact on critical infrastructures
Direct impact of the threat on the population
Population

Figure 7: Hazards can have direct and indirect consequences, which must be viewed as a whole (source: BBK 2012, p. 30, translated by: BBK).

chosen "conceivable extreme events", such as a winter storm, are described in terms of their intensity, the areas they affect, their duration, and their development.

It is possible to estimate the impact of such events on the following subjects of protection: people, the environment, the economy, and intangible property. To draw a clearer picture of the consequences, a range of different damage indicators are provided for each subject of protection. The category "people", for example, considers the number of expected deaths, people injured or taken ill, people in need of assistance or missing persons.

The consequences expected from a scenario are often closely linked to the impact the scenario is expected to have on critical infrastructures. For each scenario analysed, the first step is to calculate the impact on the CI sectors (→ Infobox 2) and to use this as a basis from which to assess the impact on the aforementioned subjects of protection. For example, it was assumed that the winter storm analysed in 2013 would also lead to regional power outages. Thus, in addition to the number of people who would need help due to the storm itself – perhaps due to injuries they may have suffered or damage to their homes – there would also be an additional group of people who would require temporary assistance due to power outages and interruptions to the drinking water supply, for instance. So interruptions to critical infrastructures need to be taken into account as part of the overall context as "indirect" consequences of an incident (cf. Figure 7) and are therefore a key part of the method used for risk analyses in the field of civil protection.

In 2011, a steering committee for the federal department (coordinated by the BMI) and a task force for the division authorities (coordinated by the BBK) were set up in order to implement the national risk analysis for civil protection at the federal level. The role of the steering committee includes selecting the threats deemed to be relevant at the federal level. Scenarios are then described and analysed for these threats in threat-specific working groups within the task force. This process sees existing insights and information being pooled and adapted to meet the methodological structure. Expertise from other sectors, e.g. from science, from regional institutions or from operators of critical infrastructures, is also incorporated into the analysis where required. This has led to the creation of a broad "risk analysis network", which is further expanded with each subsequent analysis.

2.1.4 Critical infrastructure protection as part of spatial planning

Section 2(2)(3) of the *German Spatial Planning Act* (ROG, → Chapter 2.2.1) emphasises the importance of spatial planning for preventative risk management by the principle of meeting the requirements of critical infrastructure protection. This raises questions: What weight should be given to critical infrastructure protection in spatial planning? How can the potential provided by spatial planning be maximised in preventative critical infrastructure protection?

How can critical infrastructure protection be combined with existing tasks to ensure integrated risk management (e.g. with preventative flood protection, → Infobox 4)?

In this context, preventative risk management can be used to identify threats and vulnerabilities, and to estimate the risks relevant to spatial planning and the exposure of subjects of protection to these threats. Here we are talking about the risks and threats described in Section 1(1) and Section 8(6) of the ROG, which need to be considered from a supra-local and interdisciplinary viewpoint due to their spatial impact. One key role played by spatial planning is to spatially overlap different sources and areas of risk on the one hand and existing critical infrastructures on the other. This method can be used to identify interdependencies and cumulative threats and to take these into account during the planning stages.

The "Demonstration Projects of Spatial Planning" (MORO) has proven its worth when it comes to developing and testing approaches for new spatial planning issues. Supported by the BMI and supervised by the Federal Institute for Research on Building, Urban Affairs and Spatial

Development (BBSR), which is part of the Federal Office for Building and Regional Planning (BBR), in 2013 a field of research entitled “Preventative Risk Management in Regional Planning” was established as part of this action programme. The potentials of regional planning for risk prevention were examined in an initial model planning project, paying special attention to the concerns of critical infrastructures (cf. BMVI/BBSR 2015). As part of this, an approach for integrated risk management within the context of spatial risk prevention was developed in conjunction with regional planning authorities. This approach is intended to be used when regional plans are updated or realigned.

Recommendations were made concerning the following:

- Which resources concerning the spatial distribution of hazards and vulnerable subjects of protection, in particular critical infrastructures, can be used when drawing up a regional plan?
- How can concerns about risk be accounted for in the consultation process?
- Which instruments are suitable for formulating statutory regional planning regulations with regard to critical infrastructure?
- How can public interest parties be involved (cf. Figure 8)?

The approach to risk management that focuses on the spatial situation provides a cross-sector perspective on critical infrastructure protection: it not only highlights the situation of individual infrastructures with regard to diverse threats that are relevant to regional planning, it also elucidates the situation of the individual infrastructures with regard to one another. The fact that a high density of different infrastructures located in endangered areas can massively increase the risk potential means that this point of view is extremely important. In cases such as this, applying individual, industry-specific safety regulations separately could fall short or inhibit the search for an integrated solution. In this context, spatial planning, with its cross-sectoral, interdisciplinary and balancing function, provides an opportunity to break through a purely sectoral perspective and to resolve conflicts arising from the bundling of infrastructure. One of the key findings from the model project is that there is a need for systematic information about the criticality of infrastructures, so that they can be dealt with appropriately within spatial planning and so that their resilience can be increased (→ Chapter 2.1.2).

A subsequent project involving an expansion to two further model regions – Stuttgart and Schleswig-Holstein/Planning Area I – covered a wide range of regional planning organisations and legal structures as well as addressing spatial, risk-based problems. The expertise acquired through the expansion of the concept to these model regions is to be incorporated into a revised version of the guidelines.

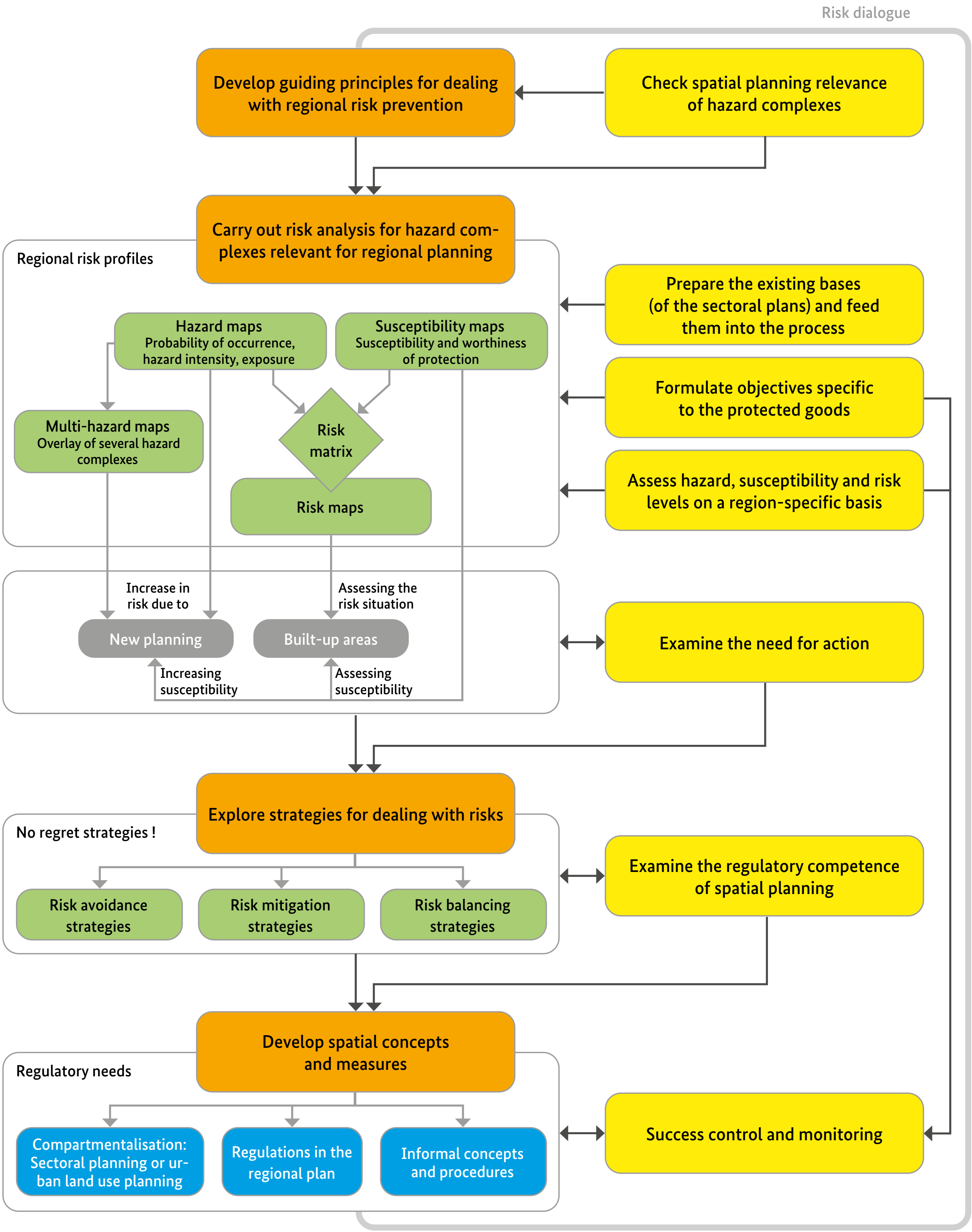
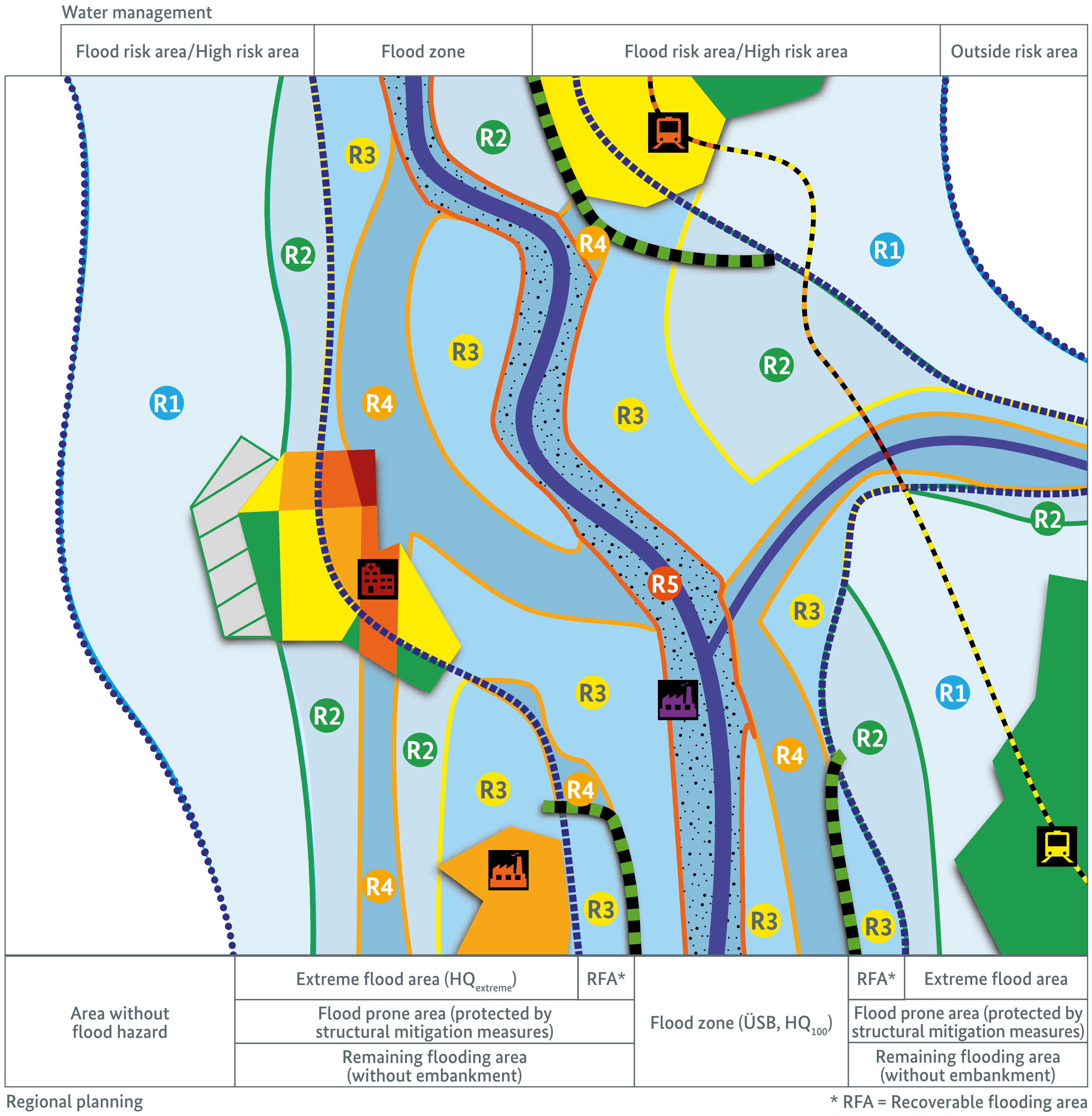

Risk dialogue
Develop guiding principles for dealing with regional risk prevention
Check spatial planning relevance of hazard complexes
Carry out risk analysis for hazard complexes relevant for regional planning
Regional risk profiles
Hazard maps
Probability of occurrence, hazard intensity, exposure
Susceptibility maps
Susceptibility and worthiness of protection
Multi-hazard maps
Overlay of several hazard complexes
Risk matrix
Risk maps
Prepare the existing bases (of the sectoral plans) and feed them into the process
Formulate objectives specific to the protected goods
Assess hazard, susceptibility and risk levels on a region-specific basis
Increase in risk due to
Assessing the risk situation
New planning
Built-up areas
Increasing susceptibility
Assessing susceptibility
Examine the need for action
Explore strategies for dealing with risks
No regret strategies !
Risk avoidance strategies
Risk mitigation strategies
Risk balancing strategies
Examine the regulatory competence of spatial planning
Develop spatial concepts and measures
Regulatory needs
Compartmentalisation: Sectoral planning or urban land use planning
Regulations in the regional plan
Informal concepts and procedures
Success control and monitoring

Figure 8: Roadmap for integrated risk management for spatial risk prevention in regional planning
(source: agl/prc, in: BMVI/BBSR 2015, p. 139; see also ARL 2011, Pohl/Zehetmair 2011, translated by: agl/prc).

Infobox 4: Spatial flood prevention with a new approach to risk?

The need for a stronger focus on risk in regional planning has also been discussed within the context of the BBSR research projects on a possible “federal spatial plan for flood protection” in accordance with Section 17(2) of the ROG. A risk approach opens up the possibility of assessing multiple spatial risks, for example reciprocal effects in the event of large-scale flooding disasters. The benefit of this systematic localisation and prioritisation is that the measures to reduce the risk can be applied in a more targeted manner. With this in mind, a practical handbook has been compiled for developing innovative approaches to state and regional planning (cf. BMVI 2017). One aspect worth highlighting from the handbook is the differentiated approach to regional risk assessment, according to which the vulnerability or sensitivity of the subjects of protection – e.g. critical infrastructures – can be processed via an integrated perspective using maps and then evaluated in a risk matrix according to several different vulnerability indicators and flood danger levels (cf. Figure 9).

The handbook includes considerations about dealing with critical infrastructures as part of regional risk prevention in two sample planning records. The first implies that, wherever possible, critical infrastructures should not be built or developed in areas at risk of flooding and, where this is unavoidable, property protection measures should be mandatory. Thus, the best-case scenario is to avoid a situation where critical infrastructures could be exposed to flooding – where this is not possible, it should at least be ensured that no damage can occur as a result. According to the second planning record, the “bundling requirement” is to be deviated from in areas at risk of flooding where structural measures do not offer sufficient protection. In most cases, the regional bundling of infrastructures is an effective way to protect nature and the landscape within spatial planning – however, in cases where several critical infrastructures could be affected by the same flooding, it represents a deeply unfavourable situation. The handbook emphasises that planning authorities must be aware which infrastructures are rated as critical in order to be able to accommodate critical infrastructure protection in the most effective possible way. As a result, the authors of the handbook consider the identification of critical infrastructures to be a crucial stage in the planning process (→ Chapter 2.1.2).


Water management
Flood risk area/High risk area
Flood zone
Flood risk area/High risk area
Outside risk area
R3
R2
R2
R4
R1
R3
R2
R1
R4
R3
R5
R3
R2
R3
R1
R2
R2
R4
R2
R3
R4
R4
R3
R3
R3
Area without flood hazard
Extreme flood area (HQ$_{extreme}$)
RFA*
Flood prone area (protected by structural mitigation measures)
Remaining flooding area (without embankment)
Flood zone (ÜSB, HQ$_{100}$)
RFA*
Extreme flood area
Flood prone area (protected by structural mitigation measures)
Remaining flooding area (without embankment)
Regional planning
* RFA = Recoverable flooding area

Risk levels

🟦 The risk levels for settlement areas and critical infrastructures are shown in two-dimensional form,

R1 For all other areas, they are marked with symbols.

Risk matrix	Susceptibility level 1	Susceptibility level 2	Susceptibility level 3
Flood hazard level 1	R 1	R 2	R 3
Flood hazard level 2	R 2	R 3	R 4
Flood hazard level 3	R 3	R 4	R 5
Flood hazard level 4	R 4	R 5	R 6
Flood hazard level 5	R 5	R 6	R 7

Figure 9: Spatial approach to risk for flood prevention – systematic sketch for risk classification for the risk of river flooding (source: agl/prc, in: BMVI 2017, p. 48, translated by: agl/prc).

2.2

Chapter

Source: Christine Müller / Westend61 / Getty Images

The operational framework for critical infrastructure protection

According to the CIP Strategy guiding policy concept, "either – primarily – as a moderator or – if required – by rule-making, the state regulates the measures for safeguarding and securing the overall system and the system procedural flows" (BMI 2009, p. 2). In line with this guiding principle, when it comes to critical infrastructure protection, the focus has been and remains on non-regulatory instruments. There is no comprehensive "law governing critical infrastructure protection" in Germany. Despite this, over time certain aspects of critical infrastructure protection have been written into specialised laws (→ Chapter 2.2.1), either to transfer regulations from the European level into German law or to cover a recognised need for regulation at the national level. Those legal regulations with an explicit link to critical infrastructure protection have a number of forms and functions: in some cases, they formulate abstract objectives, stipulate the powers of authorities or set specific requirements for operators. In particular, the *IT Security Law,* which came into force in 2015, has left its mark on many specialised laws as a so-called "omnibus" act. It made it necessary to regulate aspects of its implementation by way of additional legislation and also set in motion the development of standards for legally compliant implementation. The *Energy Industry Act* shows how the general legal framework for critical infrastructure protection is interlinked with subject-specific regulations (→ Infobox 5).

Norms and standards are used to put legal stipulations into specific terms, in particular with regard to the abstract "state of technology", which laws often refer to. They also perform this function in the context of critical infrastructure protection (→ Chapter 2.2.2). They are used in one form or another in all sectors of critical infrastructure systems, include technical specifications and describe procedures or processes. Many norms and standards aim to provide reliable and safe processes; some also expressly relate to critical infrastructure protection. Yet it is not just the passed norms and standards that have an effect: their development can lead to new topics being revealed by experts as part of the structured process, allowing for consensus to be reached.

Long before "critical infrastructure protection" became an established area of policy, the safeguarding of central utility services in defined crisis situations formed part of the statutory regulations (→ Chapter 2.2.3): the precautionary laws contain provisions for coping with supply shortages in peacetime, while the safeguarding laws are designed to deal with supply crises in the case of situations of tension or defence (Art. 80a or 115a GG).

The areas of supply addressed in these laws correspond to a certain degree to the sectors of critical infrastructure systems. One example of a legal norm, which addresses supply crises in both peacetime and in situations of tension or defence, is the law governing the *emergency control and emergency supply of food,* which was amended in 2017 (→ Infobox 6).

2.2.1 Critical infrastructure protection in federal legislation

The directive on the *Identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (2008/114/EC) was passed at the end of 2008 and came into force at the beginning of 2009. It provided the first impetus at the European level for member states to incorporate aspects of the protection of explicitly *critical* infrastructures into statutory regulations (→ Chapter 2.6.1). The directive concerns European critical infrastructures, which are understood to be "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States" (Art. 2b 2008/114/EC). The implementation of the directive prompted an initial identification process in the *transport and traffic* and *energy* sectors in Germany and led to a change of the *Energy Industry Act* (EnWG, → Infobox 5).

At the national level, the *German Spatial Planning Act* (ROG) was introduced at almost exactly the same time. A comprehensive amendment of the law at the end of 2008 ensured that the passage "critical infrastructure protection must be taken into account" (Section 2(2)(3) ROG) was included in the principles of spatial planning. Since then, the concerns of critical infrastructure protection have to be taken into account in decisions pertaining to balancing and discretionary decisions within the context of spatially significant planning and measures (cf. Section 4 ROG). Put simply, spatial planning should contribute to risk management for critical infrastructures using the means available (→ Chapter 2.1.4 and Infobox 4).

Shortly after, in 2009, aspects of critical infrastructure protection were incorporated in the *Federal Civil Protection and Disaster Assistance Act* (ZSKG). The law regulates the powers of the BBK to collate and process data concerning critical infrastructures (Section 17(1)(3) ZSKG) and also specifies the focus of civil protection in its definition: according to the law, this focus relates to "infrastructure whose disruption would significantly impair the supply of vital services to the population (critical infrastructure)" (Section 17(1)(3) ZSKG). Furthermore, the *Federal Civil Protection and Disaster Assistance Act* instructs the federal government to advise and support states with regard to critical infrastructure protection (cf. Section 18(2) ZSKG).

The *IT Security Law* (IT-SiG) came into force in 2015. Its objective was to improve the availability, integrity, authenticity, and confidentiality of IT systems, in particular with regard to IT systems used to operate critical infrastructures. In other words: critical infrastructures should be better equipped against threats spread via, as well as impacting, IT systems. As an omnibus act, the *IT Security Law* led to changes in many other laws, including the *Energy Industry Act* (→ Infobox 5), but especially in the *Act on the Federal Office for Information Security* (BSIG). It gave further responsibilities and powers to the BSI and assigned additional obligations to the operators of critical infrastructures (e.g. reporting obligations for IT security incidents or the requirement to keep their systems up to date in line with the "latest state of technology" and to be able to provide evidence of this) (→ Chapter 2.2.2).

For this purpose, it was necessary to provide a binding definition for which specific facilities are considered critical infrastructures "within the meaning of the law". In other words, it made it necessary to identify those "facilities, equipment or parts thereof which (1) are part of the sectors energy, information technology and telecommunications, transportation and traffic, health, water, nutrition, and the finance and insurance industries and (2) are of high importance to the functioning of the community since their failure or impairment would result in material shortages of supply or dangers to public safety" (Section 2(10) BSIG). The identification process for the seven regulated sectors of critical infrastructures was regulated by the *BSI Critical Infrastructure Ordinance* (BSI-KritisV) (→ Chapter 2.1.2, Chapter 2.4.2 and Infobox 16).

By the time the *Directive concerning measures for a high common level of security of network and information systems across the Union* (the so-called "NIS Directive", 2016/11487/EU) needed to be passed into German law in 2016, a foundation had already been created by the *IT Security Law* and the BSIG. The implementation act increased the powers of the BSI in line with the stipulations of the directive. Since then, the BSIG and the BSI-KritisV have also been used to determine the scope of other legal standards. For example, an amendment to the *German Foreign Trade and Payments Ordinance* (AWV), passed at the end of 2018, gave the Federal Ministry for Economic Affairs and Energy (BMWi) the option to examine company holdings in operators of critical infrastructures in accordance with BSIG, with an intervention threshold lowered from 25% to 10% (cf. Section 55 AWV).

The *Telecommunications Act* (TKG) took a slightly different approach. It was modified in 2016 with the *Law to Facilitate the Expansion of Digital High-Speed Networks* (DigiNetzG) and now contains a series of exemptions in the interests of critical infrastructure protection, mainly in a sub-section entitled "Shared use of the public utility network". It is, for example, possible to forgo the inclusion of certain information in the "Infrastructure Atlas" managed by the Federal Network Agency (BNetzA), where "parts of an infrastructure are affected, which have been designated critical infrastructures by law or as a result of legislation and that can be proven to be particularly vulnerable and that are important to the functioning of the critical infrastructure" (Section 77a(4)(3) TKG). The open wording "by law or as a result of legislation" includes the BSIG and the BSI-KritisV, as well as the *Energy Industry Act* (→ Infobox 5; cf. BT-Drs 18/8332, p. 41). Should further laws be introduced to define critical infrastructures in the future, the *Telecommunications Act* already includes a pathway to achieve this.

Infobox 5: Critical infrastructure protection on the basis of the *Energy Industry Act*

The purpose of the *Energy Industry Act* is to provide "the most secure, affordable, consumer-friendly, efficient, and sustainable supply of electricity and gas to the general public, with an increasing focus on renewable energies" (Section 1(1) EnWG). Security of the supply is clearly formulated right at the start of the legal norm and is set in stone in many other sections of the legislation. In other words, the interests of critical infrastructure protection have been taken into account in many parts of the EnWG, without there being an explicit reference to critical infrastructure protection. Furthermore, the EnWG shows how the general legal framework for critical infrastructure protection is interlinked with regulations specific to different sectors.

With the implementation of 2008 Directive 2008/114/EC in national law, the protection of *European* critical infrastructures was written into the EnWG (→ Chapter 2.6.1).

Section 12g of EnWG contains provisions relating to "facilities or parts of facilities from the power grid, the interruption or destruction of which could have a considerable impact on at least two European member states (critical European facilities)". Every two years in its role as the regulatory body, the BNetzA determines which particular facilities are considered as such and which operators need to meet the requirements formulated herein as a result.

The *IT Security Law,* passed into law in 2015, has also left its mark on the EnWG (→ Infobox 16). Section 11(1b) and (1c) of the EnWG address the operators of energy supply networks and of those energy facilities "which are defined as critical infrastructures by the commencement of the regulation in accordance with Section 10(1) of the *BSI Act*". The EnWG obliges operators to guarantee that appropriate protection is provided for threats against the telecommunications and electronic data processing systems they use (cf. Section 11(1b) EnWG). These requirements to be met by the operators are described in more detail in so-called security catalogues, which have been developed by the BNetzA in consultation with the BSI. According to Section 11(1c) EnWG, the operators must also report to the BSI any major interruptions to the availability, integrity, authenticity, and confidentiality of IT systems, components, and processes.

2.2.2 Norms and standards – a key factor in implementing critical infrastructure protection

Norms and standards supplement legal principles and stipulate generally acknowledged codes of practice. They are published by standardisation bodies, such as the German Institute for Standardisation (DIN). As registered associations, these non-profit organisations are national or international platforms providing standards. In addition, norm-like policies are published by associations with national reach, such as the Forum Network Technology/Network Operation (FNN) in the Association for Electrical, Electronic & Information Technologies (VDE), the German Association for Gas and Water (DVGW), and the German Association for Water, Wastewater and Waste (DWA). These institutes also develop generally accepted codes of practice. Norms and standards provide the opportunity to substantiate legal regulations, to stipulate uniform processes and regulations for specific industries and thus to increase the legal certainty for operators, and this is also the case within the context of critical infrastructure protection. In addition, work on norms and standards can help to generate discussions around innovative approaches to critical infrastructure protection and can serve to incorporate new perspectives into the standardisation process as a result. All norms and standards are developed by groups of experts, with the participation of members of the professional public, in a transparent process. Close cooperation between operators of critical infrastructures, associations and experts from the authorities, industry, and research serves to improve policies and, with it, to enhance critical infrastructure protection.

Norms and standards can describe and standardise procedures. For critical infrastructure protection, they address important topics such as risk and crisis management. For example, the regulation DIN ISO 31000:2018-10, entitled "Risk management – Guidelines" focuses on risk management procedures. The DIN specification DIN SPEC 91390:2019-12 "Integrated risk management in civil protection" addresses the special aspect of cooperation between state administrative bodies and local authorities with operators of critical infrastructures (→ Chapter 2.4.3 and Infobox 17). DIN specifications are not binding or obligatory in themselves, but they can lead to an actual standardisation process. Most industry-specific technical regulations include specifications for the planning, construction, and operation of particular facilities. These can be supplemented with codes of practice or information with a focus on specific scenarios, such as extreme weather events, for example. Thus, for example in the gas supply sector, a new code of practice entitled "Instructions for maintaining a secure gas supply in the event of failure of regular communications" has been drawn up (DVGW G 1003). A code of practice is currently being developed for the wastewater disposal sector, which focuses on risk assessment and how to overcome a long-lasting and extensive power cut (DWA M 320 "Ensuring wastewater disposal in the case of a power cut"). The code of practice DWA M 551: Audit "Flooding – how well-prepared are we?" looks at preparations for flooding and heavy rainfall.

The European level also plays a key role when it comes to norms and standardisation. In order to guarantee safe operation of the large European integrated networks, the European Network of Transmission System Operators for Electricity (ENTSO-E) and the European Network of Transmission System Operators for Gas (ENTSO-G) draw up "Network Codes" – binding policies for all network partners regarding network operation. Norms and standardisation processes at the European and national levels often need to be made uniform. Looking at the water supply sector as an example, guidance on risk management (W 1001) and crisis management (W 1002) for the drinking water supply was initially developed at the national level under the leadership of the DVGW. This DVGW guidance was then standardised at the European level and carried over into the norms DIN EN 15975-1 "Security of the drinking water supply – Guidelines for risk and crisis management – Part 1: Crisis management" and DIN EN 15975-2 "Security of the drinking water supply – Guidelines for risk and crisis management – Part 2: Risk management".

The increasing importance of IT security within the context of critical infrastructure protection is, as expected, also reflected in the creation of norms and standards. The BSI compiled the BSI Standards with IT baseline security in mind. They provide information about the risk analysis procedure and about emergency management amongst other things (cf. BSI Standard 200-2 “IT Baseline Security”). When it comes to operators of critical infrastructures, as described by Section 2(10) BSIG, special requirements apply regarding IT security (→ Chapter 2.2.1): according to Section 8a(1) BSIG, operators are obliged to take appropriate organisational and technical precautions to avoid interruptions to the availability, integrity, authenticity, and confidentiality of their IT systems, components or processes, which are fundamental to the functioning of the critical infrastructures they operate. The state of technology that needs to be adhered to can be set out in “industry-specific security standards” (B3S) (→ Infobox 16). Code of practice 1060 “IT security – industry standard for water/wastewater”, which was published by the DVGW and DWA, is given as an example here. In some cases, the requirements formulated in the *IT Security Law* have been integrated in special laws, e.g. in the *Energy Industry Act* and the *Telecommunications Act.* Here, “IT Security Catalogues” set out the requirements facing operators (BNetzA 2015; BNetzA 2016; BNetzA 2018). The IT Security Catalogues for the *Energy Industry Act* were compiled by the BNetzA in collaboration with the BSI, and the IT Security Catalogue for the *Telecommunications Act* was drawn up in agreement with the BSI and the Federal Commissioner for Data Protection and Freedom of Information (BfDI).

Norms and standards that contribute to critical infrastructure protection and to security of supply for the populace are constantly being developed and adapted to changing requirements by expert committees in which representatives from the respective specialist authorities offer their perspectives.

2.2.3 The legal basis for the management of supply crises

Even before critical infrastructure protection became established at the end of the 1990s, maintaining crucial utility services was an important task for the state. A series of laws concerning defined crisis situations has been passed for this purpose since the 1960s (cf. Table 4). Some of these laws concern bottlenecks in supply in peacetime – the *Precautionary Laws* – others are explicitly linked with Articles 80a or 115a of the Basic Law of the Federal Republic of Germany (Grundgesetz, or GG) and, as such, are specifically intended for situations of tension or defence – the *Safeguarding Laws.* In order to be able to apply the legislation, the federal government must generally formally stipulate the application or the parliament may need to pass a corresponding ruling. The only exceptions are those regulations concerning precautionary measures, which are to be implemented during “normal service” (e.g. building measures or the provision of certain resources).

The precautionary and safeguarding laws are intended to ensure that the basic provision of goods and services is safeguarded for both the general population and the armed forces (→ Chapter 2.3.2). With this in mind, they specify how limited resources are to be distributed in a crisis within certain sectors (→ Infobox 2). For example, the *Energy Security Act* was used as a basis to pass regulations concerning the generation and distribution of electricity in order to be able to provide for essential energy needs in the event of a shortage. The *Labour Protection Act* makes it possible to require certain groups of people to enter into required employment relationships, and most CI sectors are explicitly named as applications. When it comes to the details, the precautionary and safeguarding laws often refer to statutory instruments that are to be drawn up – possibly with the involvement of the Bundesrat – or to existing legal ordinances.

CI sector	***Precautionary and Contingency Acts***
Energy	*Energy Security Act* (EnSiG) *Petroleum Stockholding Act* (ErdölBevG) *Economic Security Act* (WiSiG)
Information technology and telecommunications	*Post and Telecommunications Security Act* (PTSG)
Transport and traffic	*Transportation Provision Act* (VerkLG) *Transport Security Act* (VerkSiG)
Water	*Water Security Act* (WasSiG)
Food	*Emergency Food Control Act* and the *Emergency Food Supply Act* (ESVG)
Finance and insurance	*Economic Security Act* (WiSiG)
Relevance to all sectors	*Labour Security Act* (ASG) *Federal Requisitioning Law* (BLG)

Table 4: Precautionary and Contingency Acts relating to critical infrastructures (compiled by: BBK).

It is not surprising to note that many of the Precautionary and Contingency Acts concern the provision of goods and services that also play a role in the protection of critical infrastructure (cf. Table 4). After all, protecting critical infrastructure is an ongoing task and should ensure that supplies are guaranteed at all times. The Precautionary and Contingency Acts supplement the legal basis in certain sectors and for defined periods of crises, so that limited resources can be best used during supply crises. To this end, they can also override market mechanisms, for example.

To ensure that the measures stipulated in the Precautionary and Contingency Acts can most effectively contribute to overcoming crises, they must be adhered to by the relevant actors at all times. As such, they are regularly the subject of exercises and training. The application of the *Energy Security Act* was, for example, practised as part of "LÜKEX 2018" (BBK 2019b; → Chapter 2.4.4). Furthermore, the Contingency Acts were checked to see if they were in need of revision as part of the implementation of the "Civil Defence Concept" (BMI 2016b; → Chapter 2.3.2). *The Post and Telecommunications Security Act* and the combined *Emergency Food Control Act* and the *Emergency Food Supply Act* (→ Infobox 6) have been revised in recent years. In both cases, the previously separate laws concerning situations of tension or defence on the one hand and peacetime crises on the other were combined to create a single law. This is intended to ensure that different causes are generally addressed with the same means, so that resources can be used more effectively. The *Water Security Act* (WasSiG) primarily concerns water supplies in a situation of defence (Section 1).

However, according to Section 8 WasSiG, it is also possible to use the facilities that have been built to fulfill the obligations stipulated in Section 2 WasSiG for purposes other than securing water in a situation of defence, assuming that the responsible authorities agree to this use (double benefit).

Infobox 6: The revision of the *Emergency Food Control Act* and the *Emergency Food Supply Act*

Prior to 2017, food in times of crisis was regulated by both the *Emergency Food Control Act* and the *Emergency Food Supply Act*. The first was intended for situations of tension and defence, the second for other crises in supply. However, both these acts contained differing regulations and were no longer up to date. With this in mind, the German Federal Ministry of Food and Agriculture (BMEL) launched several research projects to shed light on the various aspects of restructuring these regulations. The legal basis of the emergency provision of food was one aspect analysed: deficits were described and recommended changes drawn up. In addition, the “New Strategies for Emergency Food Provision” (NeuENV) project, sponsored by the Federal Ministry of Education and Research (BMBF) as part of the “Research for Civil Security” programme (→ Chapter 2.3.3), came up with recommendations for action and strategies for emergency food provision. The viewpoints of all the relevant actors – food companies, political decision-makers, charities, and the general public – were taken into account during this process.

Finally, in 2017, the two laws were combined to form the *Emergency Food Control and Supply Act* (ESVG). Since then, the ESVG has covered food security both in situations of defence and in terms of peacetime provision. The application of the ESVG is contingent on the federal government declaring that there is a supply crisis. However, it also features stipulations regarding provision prior to the declaration of a supply crisis. For example, it obliges the federal and regional governments to enhance the population’s resilience to withstand the consequences of a supply crisis and to find out more about individual preventative measures (cf. Figure 10). This is achieved through an online portal (www.ernaehrungsvorsorge.de) provided by the Federal Office for Agriculture and Food (BLE) as well as an information stand at “International Green Week” in Berlin, for example.

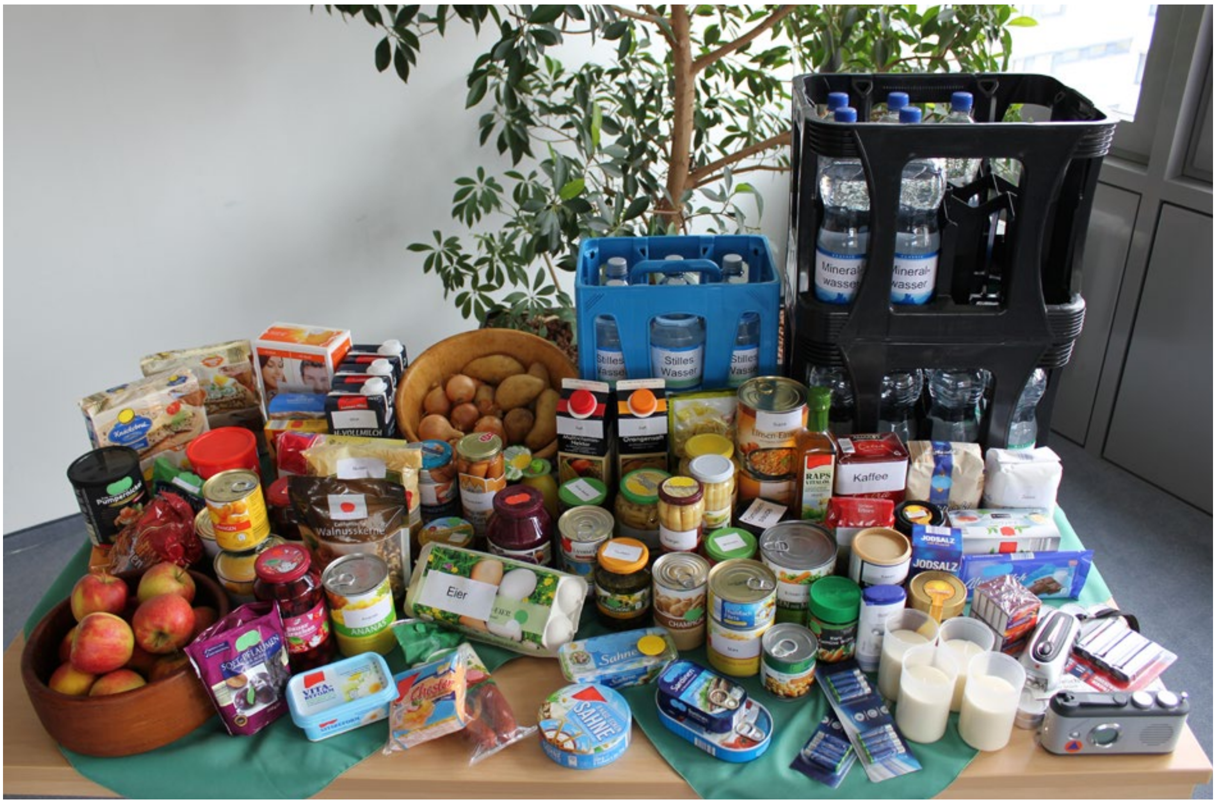


Figure 10: Example of emergency supplies for the public (source: Lechner / BBK).

2.3

Chapter

Source: Volker Pape / EyeEm / Getty Images

Critical infrastructure protection as a cross-sectoral issue

Critical infrastructure protection intersects with other fields of policy in a multitude of areas. As a result, aspects of critical infrastructure protection also appear in other political strategy documents and are addressed within that context (→ Chapter 2.3.1). Some of the relevant strategies focus on specific parts of the hazard spectrum, while others focus on a sector or industry. The "Sendai Framework for Disaster Risk Reduction" (UN 2015) covers a wider perspective. It embraces the entire All-Hazards Approach and views critical infrastructure protection as part of society's overall disaster risk reduction.

The "Civil Defence Concept" (BMI 2016b) maps out the civil part of the overall defence concept. In other words, it focuses on threats that could occur in conjunction with armed conflicts and hybrid threat situations (→ Chapter 2.3.2). Aspects of critical infrastructure protection are an integral part of the concept and therefore arise at various points. Guidelines for maintaining state and governmental functions can, for example, be viewed as threat-specific measures for critical infrastructure protection within the *state and administration* sector (→ Infobox 11).

In order to be able to promote the furthering of scientific knowledge about the value of critical infrastructure protection (→ Chapter 2.3.3), an entire pillar of the "Research for Civil Security" (BMBF 2018) programme is dedicated to this topic. Operators, such as authorities and organisations with a security remit or operators of infrastructure companies, are closely involved in all the research projects to ensure that solutions developed are feasible and fit for purpose. Furthermore, societal, legal, and ethical questions are considered from the outset. The federal government's research programme on IT security promotes research projects relating to critical infrastructure protection with a specific focus on IT security.

2.3.1 Critical infrastructure protection in political strategies

Critical infrastructure protection addresses infrastructures that are vital to society across nine sectors or 29 branches (→ Infobox 2) and follows the All-Hazards Approach, which assumes that no type of threat can be fully ruled out (→ Chapter 1.2). Critical infrastructure protection shares this broad scope of topics with a number of other political fields. This can, for example, be seen in the fact that strategy documents from other areas of policy address critical infrastructure protection, for example by dealing with one particular part of the All-Hazards Approach in detail or by taking an in-depth look at a number of sectors or branches.

The "threat-specific" strategies with a close link to critical infrastructure protection include the "Cyber Security Strategy for Germany" (CSS, BMI 2016a), which considers cyber threats. These threats can spread and impact IT systems, which are prevalent in all sectors of critical infrastructure systems (→ Infobox 7). A whole series of different phenomena from the range of natural threats play a role in the "German Strategy for Adaptation to Climate Change" (DAS, BReg 2008) (→ Infobox 8). On the one hand, CSS and DAS have a narrower focus than the CIP Strategy (BMI 2009) with regard to the range of threats. On the other, critical infrastructures are just one part of the focus of CSS and DAS. As such, there is a definite crossover between all three strategies; however, they all deal with this overlap in a different way.

The "Security Strategy for the Freight Transport and Logistics Industry" (BMVI 2014) is one example of a branch-specific strategy document that directly relates to critical infrastructure protection and the CIP Strategy. It sets out what critical infrastructure protection means for freight transportation and the logistics sector. The focus of the CIP Strategy encompasses the "Security Strategy for Freight Transportation and the Logistics Sector"; however, the CIP Strategy cannot provide the same depth required to meet the needs of individual branches due to its cross-sectoral perspective (→ Infobox 9).

The United Nations' "Sendai Framework for Disaster Risk Reduction 2015-2030" (UN ISDR 2015) encompasses critical infrastructure protection. Like the CIP Strategy, the Sendai Framework also follows an All-Hazards Approach. At the same time, the framework is not limited to the scope of critical infrastructure protection. It addresses critical infrastructure protection as one of many aspects of society's overall approach to disaster risk reduction. From this perspective, critical infrastructure protection is *one* of the building blocks required to achieve a resilient society (→ Infobox 10).

Infobox 7: The "Cyber Security Strategy for Germany"

The first seedlings for a Cyber Security Strategy were planted in 2005 with the "National Plan for Information Infrastructure Protection (NPSI; BMI 2005b), where the focus was still decidedly on protecting IT and information infrastructures (→ Chapter 1.1). The NPSI highlighted the importance of secure information infrastructures for Germany's inland security and obliged the state and private industry to contribute to improvements to the level of IT security. The NPSI was accompanied by two implementation schemes. The first was aimed at the federal administration, the "Federal Implementation Plan" (current version: BMI 2017). The second, the "CIP Implementation Plan" (BMI 2007a), is predominantly intended for operators of critical infrastructures, as well as specialist associations and the responsible authorities. This led to the creation of UP KRITIS as a collaboration between the state and private industry (→ Chapter 2.4.2).

In 2011, the NPSI was replaced by the "Cyber Security Strategy for Germany" (CSS, BMI 2011b). As had been the case with the NPSI, the"protection of critical information infrastructures" and the "strengthening of IT security in public administration" explicitly addressed operators of critical infrastructure protection and state authorities, while also reaching out to small and medium-sized businesses. Organisationally the architecture for cyber security was supplemented with the National Cyber Response Centre, a collaborative platform for the federal authorities that deal with cyber security, and the National Cyber Security Council, comprised of seven departments and the Federal Chancellery. For the first time, consideration was also given to implementing regulatory instruments, and this led to the *IT Security Law* being passed in 2015 (→ Chapter 2.2.1 and Infobox 16).

In 2016, the CSS was updated against the backdrop of the qualitative and quantitative progress of digitalisation (BMI 2016a). It had the aim of guaranteeing Germany's sovereignty and ability to act in the age of digitalisation, of using the opportunities and potentials offered by digitalisation and of mastering the associated risks. Four action areas were defined for this purpose and corresponding strategic objectives and measures outlined:

1. Remaining safe and autonomous in a digital environment
2. Government and private industry working together
3. Strong and sustainable cyber security architecture for every level of government
4. Germany's active role in European and international cyber security policy

Critical infrastructure protection was addressed in the CSS as "government and private industry joint order" in the action area of the same name. The promotion of close and trusting cooperation across all levels, as had been described in the NPSI, is accompanied by preventative measures, such as developing and implementing minimum standards, as well as response obligations, such as stipulating reporting channels.

Infobox 8: The "German Strategy for Adaptation to Climate Change"

It is already clear that climate change is affecting life in Germany and will continue to do so in the future. To respond to this, in terms of reducing vulnerabilities and maximising opportunities for adaptation, in 2008 the federal government passed the "German Strategy for Adaptation to Climate Change" (DAS) (BReg 2008). As a result of the importance of the infrastructures and the services that they help to provide, it comes as no surprise that many of the DAS action areas correspond with critical infrastructure sectors, for example the water sector, the energy sector as well as financial services. Civil protection – like spatial, regional, and urban land use – is considered a cross-sectoral issue in the DAS due to its multiple links to the various spheres of action.

The evolution of a wide range of natural threats – from heatwaves to heavy rainfall – can be seen as a result of climate change. Measures to increase the resilience of critical infrastructure systems to these threats are equally relevant to adaptation to climate change *and* critical infrastructure protection. Identifying and exploiting these links offers progress for both processes – and this was also the conclusion drawn by the DAS progress report (BReg 2015). This is why everyone dealing with critical infrastructure protection should take a look at the "German Climate Preparedness Portal" (www.klivoportal.de), which brings together the services provided by the federal and regional governments for a targeted adaptation to the consequences of climate change. Many of the services available on the portal can make important contributions to risk management for critical infrastructures. Both the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) and the KomPass competence centre for "Climate Impacts and Adaptation in Germany" (KomPass), supported by the German Environment Agency (UBA), provide further information about implementing the DAS.

Infobox 9: The "Security Strategy for the Freight Transport and Logistics Industry"

The CIP Strategy summarises the federal government's objectives and strategic political approach for critical infrastructure protection as a whole. With the "Security Strategy for the Freight Transport and Logistics Industry" (BMVI 2014), the Federal Ministry of Transport and Digital Infrastructure (BMVI) has laid the foundations for implementing this strategy in the *transport and traffic* sector (→ Infobox 2). The Security Strategy aims to prevent long-term disruptions and outages to infrastructure caused by external influences that can lead to severe disruptions to the goods supply of the general population and private industry and, in the event of an incident, to build the capacity to deploy effective crisis management quickly and appropriately.

The Security Strategy picks up on many of the general approaches and implementation steps described in the CIP Strategy for critical infrastructure protection, while providing a branch-specific perspective. One example is that of the continued and deeper collaboration between state and private actors as one of the main objectives of the Security Strategy. The "Security in Logistics" working group, which was launched prior to the development of the strategy, serves to bring these groups of actors together, support the implementation of the strategy and develop it on an ongoing basis. It is closely linked with the UP KRITIS *transport and traffic* branch working group → Chapter 2.4.2). In addition, emphasis is placed on the importance of exercises involving state authorities and operators, as well as on the commitment of actors from the *transport and traffic* sector to the series of exercises known as LÜKEX (→ Chapter 2.4.4).

Infobox 10: The “Sendai Framework for Disaster Risk Reduction”

National Focal Point
for the Sendai Framework
Germany

The Third UN World Conference on Disaster Risk Reduction took place in Sendai (Japan) in March 2015, resulting in 187 states adopting the “Sendai Framework for Disaster Risk Reduction 2015-2030” (cf. UN 2015). Through its implementation, nations strive to achieve the substantial reduction of disaster risk and losses in all areas across the globe by 2030. The goal is to reduce existing risks and vulnerabilities, to prevent new disaster risks and to increase the population’s resilience to natural or human-made disasters.

To support assessment of this goal, the Sendai Framework outlines seven global targets that aim to substantially reduce (a) global disaster mortality, (b) the number of affected people, (c) economic loss and (d) “damage to critical infrastructure and disruption of basic services”. In addition, (e) the number of countries with disaster risk reduction strategies should be increased, (f) international cooperation should be enhanced, and (g) the availability of multi-hazard early warning systems and disaster risk information should be increased (UN 2015, p. 12).

To achieve these targets, the Sendai Framework sets four priorities for action (UN 2015, p. 14):

1. Understanding disaster risk

2. Strengthening disaster risk governance to manage disaster risk

3. Investing in disaster risk reduction for resilience

4. Enhancing disaster preparedness for effective response and to “Build Back Better” in recovery, rehabilitation, and reconstruction.

Germany has also adopted the Sendai Framework, which involves implementing it in the country as well as contributing to meeting the global targets through international cooperation. The implementation process is controlled by an inter-ministerial working group. In 2017, the Office of the National Focal Point for the Sendai Framework (NKS) was set up within the BBK to coordinate implementation and provide technical support.

The links between the objectives of the CIP Strategy (BMI 2009) and the targets described in the Sendai Framework of “substantially reducing disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities”, as well as “developing their resilience” (UN 2015, p. 12) are particularly noticeable. Yet, the ability to reduce the number of victims of and people affected by disasters and the degree of economic damage caused by these disasters are also highly dependent on how well infrastructure services can be supplied during disasters or how quickly they can be made available again should they be disrupted. Critical infrastructure protection is a vital aspect of reducing disaster risk, and the CIP Strategy is a key component in implementing the Sendai Framework in Germany.

2.3.2 The role of critical infrastructure protection in the “Civil Defence Concept”

According to the All-Hazards Approach described in the CIP Strategy (BMI 2009), a range of different threats should be considered when it comes to critical infrastructure protection. These threats include those that may arise in conjunction with armed conflicts. As such, critical infrastructure protection also plays a role in the “Civil Defence Concept” (KZV, BMI 2016b), which was enacted by the federal cabinet in 2016. The KZV includes guidelines about the areas of civil defence shown in Figure 11: “ensuring the continuity of state and government functions”, “protecting the public”, “providing goods and services” and “helping the armed forces”. Furthermore, the seven “Baseline Requirements” for civil protection (→ Chapter 2.6.3), formulated by the North Atlantic Treaty Organization (NATO), are set out for Germany. The KZV hence forms the civil counterpart to the “Bundeswehr Concept” (BMVg 2018), and its scope for action is similarly based on the assumptions made in the “Bundeswehr White Paper” (BMVg 2016).

Civil defence and military defence are inextricably linked parts of an overall defence system (cf. Figure 11). Within this context, preparations are made for civil protection and to defend Germany, particularly in situations of tension and defence (Art. 80a(1) GG, Art. 115a GG), taking into account Germany’s obligations to the alliance (Art. 5 NATO Treaty) and in cases where mutual defence is called for (Art. 42(7) EU Treaty). The availability of critical infrastructures plays a key role in all the areas of civil defence addressed by the KZV. As such, guidelines to maintain state and governmental functions can, for example, be viewed as threat-specific measures for critical infrastructure protection within the CI sector of *state and administration* (→ Infobox 11). The field of “civil protection” largely concerns the capabilities of the *emergency and rescue services* and the *health* sector (e.g. incident notification and response planning in hospitals; → Chapter 2.5.4). The “helping the armed forces” area encompasses the provision of energy, food, and transport services. Meanwhile, the “providing goods and services” part concerns “preventing and managing the failure or disruption of goods and services”, whereby all the emergency planning described in the KZV should be based on the “existing peacetime structures and crisis preparedness measures” (BMI 2016b, p. 42). Many of the services addressed in “providing goods and services” show clear parallels to the CI sectors, for example medical care, energy supply or the (emergency) supply of water and food (→ Infobox 6).

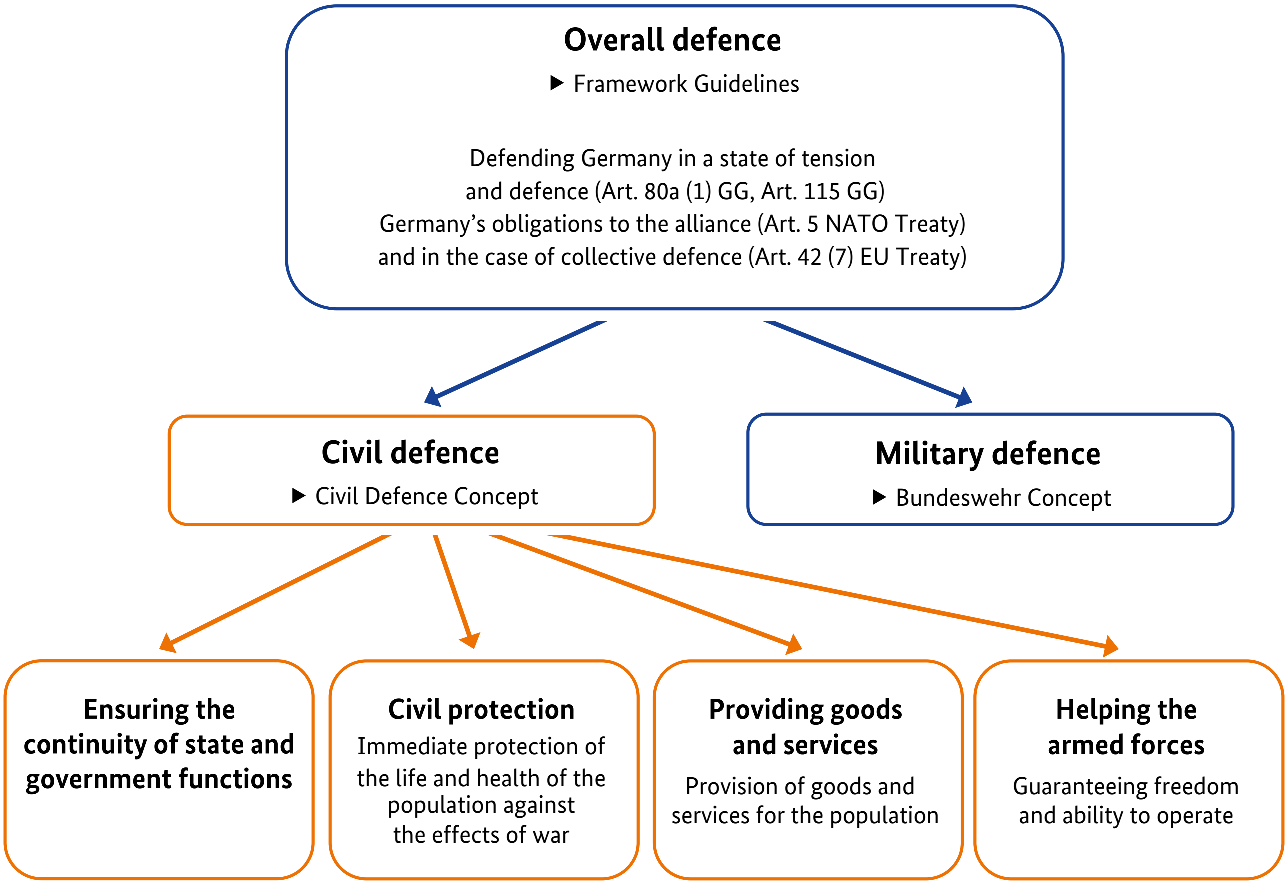

Overall defence
▶ Framework Guidelines
Defending Germany in a state of tension
and defence (Art. 80a (1) GG, Art. 115 GG)
Germany’s obligations to the alliance (Art. 5 NATO Treaty)
and in the case of collective defence (Art. 42 (7) EU Treaty)
Civil defence
▶ Civil Defence Concept
Military defence
▶ Bundeswehr Concept
Ensuring the continuity of state and government functions
Civil protection
Immediate protection of the life and health of the population against the effects of war
Providing goods and services
Provision of goods and services for the population
Helping the armed forces
Guaranteeing freedom and ability to operate

Figure 11: Areas of overall defence and the topics covered by the Civil Defence Concept (source: BBK, translated by: BBK).

The KZV considers special challenges concerning being prepared for a crisis. This includes the planning horizon: whereas in the case of a short-term crisis, non-time-critical tasks can be put on hold until the crisis has been dealt with; in a situation of tension or defence, a long-term change to the "normal state of affairs" may occur. Furthermore, extraordinary threats need to be planned for, for example arising from the use of weapons of war and the associated damage, as well as from the targeted use of the means of hybrid warfare against critical infrastructures. The

Infobox 11: Ensuring the continuity of state and government functions

The state must remain functional in a crisis situation. This does not just apply to purely peacetime scenarios; it also applies to situations of tension, defence or collective defence. In these eventualities, parliaments need to be able to pass laws, courts need to pass verdicts, and the government and administration need to be able to fulfill their duties. This is a legitimate expectation of the state and is how it is viewed by the constitutional order. As such, the areas of responsibility concerning "ensuring the continuity of state and government functions" sees the CI sector *state and administration* (→ Infobox 2) anchored in civil defence requirements. The aim of the regulations is to ensure that state organs can continue to fulfill their duties and functions, even during crises such as a situation of tension or defence. The authorities and institutions can look to their preparations for a civil crisis (emergency/crisis management); but also need to take the particularities of the situation into account (for example, how long the situation is likely or expected to last compared to peacetime crises). As such, specific questions arise in the following areas regarding ensuring the continuity of state and government functions:

1. **Changes to responsibilities**
   Is it necessary to adjust the quality and/or quantity of the tasks performed? What additional tasks are required that do not need to be performed during peacetime? Which tasks can be dropped?

2. **Organisational procedures**
   Do organisational/business distribution plans need to be adapted to changes in the way tasks are performed? Have the required points of contact with other authorities and the reporting channels been defined? Is there a special need to protect critical sectors?

3. **Technical construction measures**
   Are special building reinforcement measures required (for instance, in view of the possible use of weaponry)? Do special-access security systems need to be set up?

4. **Self-defence for authorities**
   Do special protection measures need to be taken for employees in the case of defence scenarios (e.g. occupational safety, fire protection, health measures)?

5. **HR measures**
   Which employees are key workers? Is there personnel planning for areas relevant to defence? Do exemptions or required employment relationships as described in the *Labour Protection Act* (→ Chapter 2.2.3) need to be prepared?

6. **Alternate location planning?**
   Do certain tasks need to be carried out at a protected location?

operators of infrastructure are also responsible for providing utility services and for the security of their facilities within the context of civil defence, although regionally based emergency planning within the context of crisis management plays a greater role here. Until a larger interruption to supplies can be returned to normal, local crisis management measures should be taken, as stipulated in the Precautionary and Contingency Acts (→ Chapter 2.2.3). At the same time, critical facilities can be offered special physical protection by regional police forces, with additional support being provided by the federal police if required and, under certain conditions, by the Bundeswehr.

The following applies in this scenario: "ongoing protection of critical infrastructures is a basic prerequisite for emergency preparedness within the framework of civil defence" (BMI 2016b, p. 42). Since it was passed, the KZV has prompted many actors to take extraordinary scenarios into consideration. This in turn also benefits the "peacetime" protection of critical infrastructures.

2.3.3 Research on critical infrastructure protection

Science and research can make a key contribution to increasing the resilience of critical infrastructures to disruptions and attacks and can help interruptions be resolved more quickly. This is why the Federal Ministry of Education and Research (BMBF) uses research programmes to systematically promote projects offering new insights and integrated solutions and in which new technological approaches can be developed. Issues concerning critical infrastructure protection feature in several different funding programmes – the "Research for Civil Security" framework programme and the research programme on IT security entitled "Self-determined and Safe in the Digital World" are especially relevant here.

The "Research for Civil Security" framework programme

The first civil security research programme (SiFo) was enacted in 2007 by the federal government to promote interdisciplinary research projects developing integrated solutions for increasing the security of citizens. The programme is currently in its third phase. In order to ensure the practicality of the solutions developed, practitioners – such as authorities and organisations responsible for safety and security as well as the operators of infrastructure – are closely involved with all research projects. Furthermore, relevant societal, legal, and ethical questions are considered from the outset.

Of the five funding guidelines published for the first programme in 2007/2008, two were dedicated to critical infrastructure protection. Since then, the topic has been addressed from new angles and is also one of the three central pillars in the federal government's current framework programme entitled "Research for Civil Security 2018-2023" (cf. BMBF 2018; Figure 12). The "critical infrastructure protection" programme supports projects which research integrated security solutions to increase the protection and resilience of critical infrastructures. The focus is on the *energy, health, water, food, transport and traffic,* and *media and culture* sectors (→ Infobox 2).

Since 2007, the BMBF has funded 83 research projects with a total of around 180 million euros through the "critical infrastructure protection" pillar of the programme. Below it is only possible to give a selection of the topics covered by these projects. To see a complete overview of the projects that have been funded by the "Research for Civil Security" programme, please see the BMBF website (www.sifo.de) (complete titles of the research projects given below as an example from p. 110).

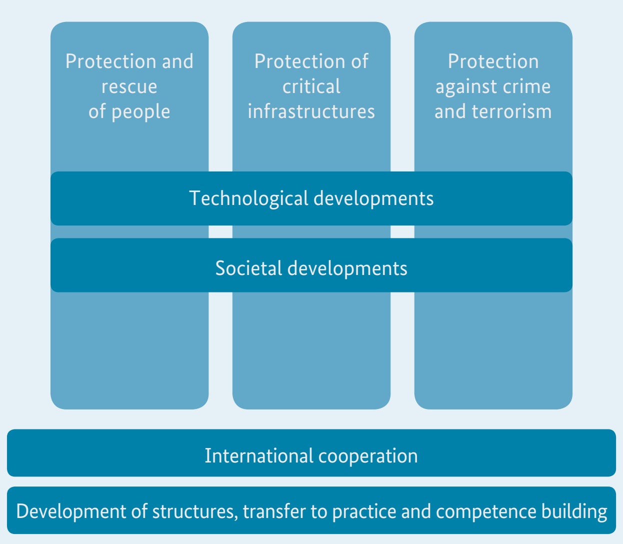

Protection and rescue of people
Protection of critical infrastructures
Protection against crime and terrorism
Technological developments
Societal developments
International cooperation
Development of structures, transfer to practice and competence building

Figure 12: Programme pillars and cross-cutting topics under the "Research for Civil Security 2018-2023" framework programme (source: BMBF 2018, Research for Civil Security 2018-2023, p. 5, translated by: BMBF).

Infobox 12: Safeguarding vital lifelines: energy and water

Power cuts may be rare in Germany, but when they occur and last for sustained periods, they can blindside private industry and the populace and can lead to severe damage. Researchers and operators of critical infrastructures are working together in research projects to find out what needs to be done when there is no electricity for a longer period due to an emergency (→ InfoStrom).

Thanks to the results of research projects like this one, funded by the BMBF, rescue and emergency staff in February 2019 were able to respond more quickly and efficiently to a power cut that deprived around 30,000 households in Berlin's Köpenick district of power for 30 hours. The Berlin fire brigade was better prepared for providing the population with the necessary information and evaluating which patients required ventilators in the case of a failure to the emergency power supply. This was in large part a result of clearly defined procedures (→ AlphaKomm; → Kat-Leuchttürme). The fire service successfully implemented a system that had been developed in a research project for monitoring the fuel supply to their emergency generators (→ TankNotStrom).

Access to a clean supply of drinking water should be a matter of course. To ensure that water is potable, a research team has developed new compact sensors that can quickly detect a wide range of hazardous substances – particularly biological or chemical. Furthermore, far-reaching emergency concepts have been compiled to increase resilience in crisis situations, and guidelines for drinking water suppliers and authorities have been developed that will contribute to the emergency services and authorities being able to respond more quickly to crisis situations. (→ AquaBioTox; → STATuS; → ResiWater).

Figure 13: (Source: Thomas Schelagowski / EyeEm / Getty Images)

Infobox 13: Guaranteeing continuous supply chains: food and health

How are the supplies of key goods, such as food and medication, to be safeguarded in crisis situations? The objective of the research is to develop innovative prevention and communication strategies, so that different actors can operate appropriately in crisis situations. These strategies include identifying harmful food contaminations at an early stage, for example. Results from civil security research allows authorities and supply companies to detect pathogens swiftly and systematically. This makes it possible to trace back in real time at which point in the supply chain the food was contaminated with an identified pathogen, so that appropriate countermeasures can be taken immediately (→ SiLeBAT; → NeuENV; → RESCUE IT).

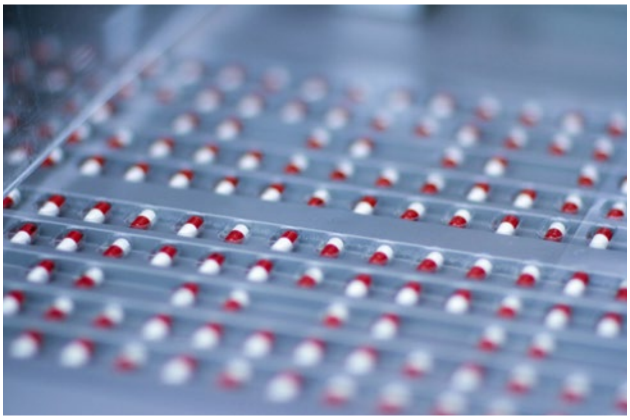


Figure 14: (Source: Sigrid Gombert / Cultura / Getty Images)

Around a third of people in Germany take regular medication to treat chronic conditions. The need for medication must be met, even in crisis situations and emergencies such as pandemics. For cases like this, scientists have developed software that reveals possible threat scenarios for the medication supply chain in advance and offers specific prevention and protection measures to all parties involved. As fake medication represents a growing threat, one research project has developed a portable chemical-testing kit to rapidly identify counterfeit drugs, for example during raids (→ MIME; → SafeMed).

Infobox 14: Creating the foundation for safe mobility: transport and traffic

830,000 kilometres of road, 38,000 km of rail, 7,300 km of waterways and 24 major airports in Germany serve to guarantee the mobility of the country's citizens. At the same time, they are a pre-requisite for the smooth supply of food, goods, and raw materials to people and businesses. Despite this, the intensity of the current volume of traffic was not always taken into account during their planning and construction.

So, researchers are working on innovations, for example using drones or other high-precision radar instruments, to calculate the current condition of bridges quickly and comprehensively (→ AISTEC; → ZEBBRA). Computer simulations can be used to identify possible damage caused by ageing and to predict further wear and tear. New technologies will also be used to monitor the structure of tunnels in real time, for example using radio sensors integrated into pieces of concrete. The data acquired is then incorporated into situation assessment systems for rescue and evacuation measures, so that extensive information about the degree of damage and condition of the structure can be sent directly to emergency response personnel in the event of an emergency (→ AISIS; → AURIS).

To identify or analyse possible safety weaknesses on ferries for different threat scenarios, a computer program has been developed. In 2014, a risk analysis procedure from a previous project was adopted by all German states with harbour facilities (→ VESPER; → VESPER^{PLUS}). A further project has simulated which damages and consequences different threat scenarios would have on artificial waterways. These simulations can be used to highlight potentially critical sections of the waterway network and to develop targeted protection measures and crisis plans (→ PREVIEW).

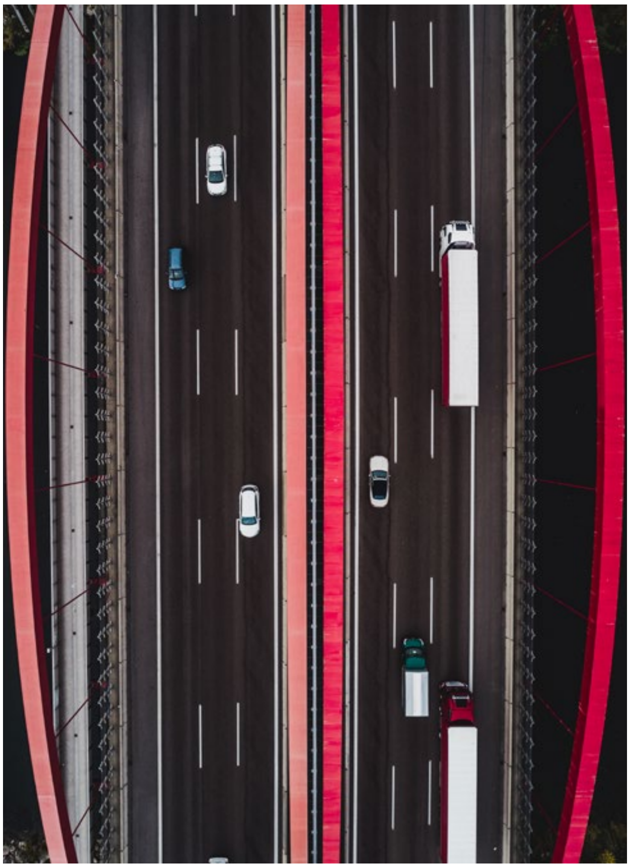


Figure 15: (Source: Abstract Aerial Art / DigitalVision / Getty Images)

Airports are particularly sensitive hubs in global travel and freight transport and are susceptible to interruptions. A body scanner has been developed as part of the civil security research programme, which uses extremely high frequency technology to detect potentially threatening items – whether liquid, metal or non-metallic. At the end of the project, the company involved brought the body scanner to market and was awarded a contract for equipping German airports with 300 body scanners (→ QPASS).

Modern security solutions are also required in the field of air freight. A system has been developed which uses radio-frequency identification (RFID) chips to monitor freight across its entire journey through the transport chain without contact, for instance to identify manipulation or tampering at an early stage (→ ESecLog).

As logistical hubs, freight villages (FV) play a key role in the supply of goods in Germany. Researchers and practitioners have developed an emergency concept designed to facilitate the emergency operation of FVs in the event of damage. This centres on a digital simulation model that visualises damaging situations and the development of damage and offers fast, automated decision-making support for relevant parties (→ PREPARED$^{\text{NET}}$).

The "Self-determined and Safe in the Digital World" framework programme

The federal government's research programme on IT security (2015-2020) bundles activities carried out across different departments regarding IT security research and promotes the development of secure, innovative IT solutions for citizens, private industry and the state (BMBF 2015).

The programme has four key areas: aside from the development of new high-tech technologies for IT security, the focus is also on secure and trustworthy information communication technology systems, IT security applications, privacy, and data protection. The framework programme has a total budget of 180 million euros.

The funding focus "IT Security for Critical Infrastructures" lies within the key area of IT security applications. It is designed to account for ongoing developments, such as growing levels of digitalisation, computer-supported process automation, and the increasingly close linking between the IT systems used by operators of critical infrastructures. These developments are vital for economic and technological reasons but they also carry risks. As such, the defined goal of the funding focus is to develop security solutions for critical infrastructures and thereby to address their everyday practicality, operability, and cost-efficiency. The strengthening and upgrading of existing systems should be valued as highly as the question of whether the solutions and methods are applicable for small and medium-sized operators.

By the end of 2018, the BMBF had provided 24 million euros of funding to eleven research consortia with this objective in mind. The "IT Security for Critical Infrastructures" funding notice involved 17 operators from the sectors *health, energy, transport and traffic, water, finance and insurance,* and *state and administration* (→ Infobox 2). The focus was on "New Approaches for Assessing IT Security" and "New Approaches for Increasing the Level of IT Security" for critical infrastructures. The range of topics addressed by the projects spans from tools to help rapidly assess and improve existing security structures (with a focus on small and medium-sized operators), to research into new procedures to detect anomalies in industrial networks, to the evaluation of IT security in view of the security awareness of the user. A comprehensive overview of the funded projects can be found on the BMBF's website under "The Communication and Security of Digital Systems".

Infobox 15: Insights into the funding priority "The IT Security of Critical Infrastructures"

The first focus, "New Approaches to Assessing IT Security", saw the development of rapid security tests for small waterworks (→ AQUA-IT-Lab), as one example. These self-assessments allow for an analysis of the current level of security and place them in relation to the industry standard and other regulatory stipulations. A test environment recreates the IT infrastructure of a typical water supplier, allowing penetration testing and realistic training for operational staff.

As part of the second focus, "New Approaches to Increase IT Security", a novel network component was developed for large power stations (→ INDI). This component is able to record data communication in sensitive areas of process technology without any lag in reaction time and to analyse anomalies. The project combined the use of systems for "Network Intrusion Detection" with machine learning and procedures to automatically analyse industrial communication protocols in a highly critical environment.

Cross-sectoral aspects of the entire funding focus, such as issues arising from the fields of law, standardisation, training, and education and innovative processes, were considered in a parallel research project (→ VeSiKi). This led to a unique compilation of all of the relevant norms and laws for operators from all CI sectors being published in the "IT Security NAVIGATOR" project (www.security-standards.de; → Chapter 2.2.2). This "meta" project was tasked with integrating those involved in the project with the CIP Implementation Plan (→ Chapter 2.4.2), taking an overarching perspective on issues concerning "IT Security for Critical Infrastructures" and supporting the transfer of results to operators. Results from this project were then compiled as a report on "State of the Art" for the IT security for critical infrastructures (cf. Rudel /Lechner 2018) and presented to the BSI at the IT security trade fair "it-sa". Both the report and a summary of case studies have been published and are freely accessible (cf. Lechner et al. 2018). There is an overview of the joint projects within the funding priority "IT Security of Critical Infrastructures", as well as other information, on the accompanying research project's website (www.itskritis.de); the full titles of the research projects cited can be found from p. 110).

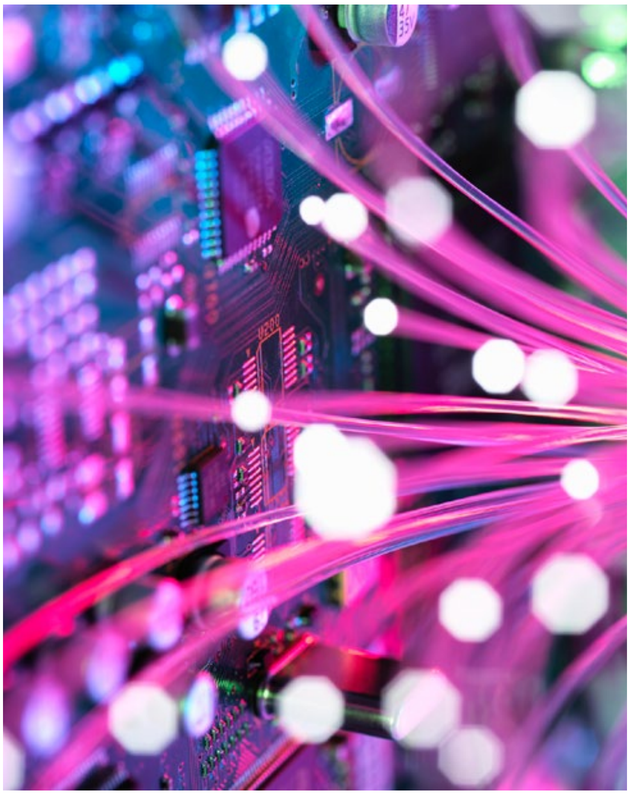


Figure 16: (Source: Andrew Brookes / Cultura / Getty Images)

2.4

Chapter

Source: Mihajlo Maricic / EyeEm / Getty Images

Critical infrastructure protection – a task requiring cooperation between various actors

The CIP (Critical Infrastructure Protection) Strategy states that "in order to strengthen critical infrastructure protection, the requirement is for intensive cooperation, coordination and information between and among the relevant partners and players" (BMI 2009, p. 12). This is due to the highly diverse range of actors involved in critical infrastructure protection: responsibilities are shared between operating companies and state bodies; technical jurisdictions are spread across various departments; supervision is conducted by authorities at various administrative levels; the operators of critical infrastructures are organised in a number of different associations; different research institutes focus on various aspects of protecting critical infrastructures – and this does not even begin to cover the many groups of actors listed under "cooperative approach" in the CIP Strategy (→ Chapter 1.2). Over time, those involved have fulfilled the mandate to work together in a variety of ways.

Critical infrastructure protection is viewed as a collective national task. Cooperation between federal government and state bodies plays a pivotal role and the creation of associated structures is a key step forward in implementing the CIP Strategy (→ Chapter 2.4.1). At the time the CIP Strategy was adopted, critical infrastructure protection was also anchored in the updating of the "Internal Security Programme" at the Standing Conference of State Interior Ministers and Senators in 2008/2009 (IMK 2009). This programme also considers an intensification of the cooperation between all state levels to be a necessity. Regular informal meetings have been taking place between the federal and state interior ministries since 2012. These meetings have proven their worth as a platform for exchanging views on cross-level issues of critical infrastructure protection and will be more closely linked to the formal committee structure of the interior ministries in future.

When it comes to critical infrastructure protection, the cooperative partnership between state authorities and predominantly private sector operators is highly valued. This is expressed in institutional terms through UP KRITIS (→ Chapter 2.4.2). On the one hand, collaboration between operators of critical infrastructures, their associations and the responsible state bodies in the UP KRITIS framework is expressed through a structured sharing of information about cyber security incidents, anomalies, and the current level of IT threat (operational and tactical cooperation). On the other hand, relevant issues specific to certain industries are investigated in working groups organised both by industry and by topic (strategic and conceptual cooperation).

When it comes to implementing the *IT Security Law*, UP KRITIS acts as an interface between state bodies and the operators of critical infrastructures (→ Infobox 16). UP KRITIS fulfills this role by developing the legal regulations used to identify critical infrastructures as defined by law. The UP KRITIS industry working groups were the first port of call when the specialist expertise of the authorities and operators needed to be brought together in "core teams" in order to tailor the parameters of the regulation so that they could be applied to specific industries. In addition, the UP KRITIS industry working groups have proven to be an ideal environment in which to develop "industry-specific security standards". With their help, it has been possible to put the stipulations of the *IT Security Law* into concrete terms for specific users in accordance with "the latest state of technology" (→ Chapter 2.2.2).

Collaboration between civil protection actors and the operators of critical infrastructures is decisive – in terms both of minimising risk and of crisis management. That is why the so-called "integrated risk management" procedure supplements the respective individual perspectives of the actors to provide an overall view, and places the focus on the interfaces and the mutual exchange of information, findings and results (→ Chapter 2.4.3). The procedure, which has now been tested multiple times in terms of its practical suitability, has recently been formalised in a DIN specification. The CIRMin research project (Critical Infrastructures Resilience as a Minimum Supply Concept) has contributed to the development of integrated risk management (→ Infobox 17).

The Interstate and Interministerial Crisis Management Exercise (LÜKEX) focuses on the interplay between crisis management performed by the operators themselves and by the authorities (→ Chapter 2.4.4). Extraordinary crisis scenarios are used to put representatives from the state authorities and operators of critical infrastructures in extremely challenging situations that call for close and sustained interaction. The aim is to develop the skills of employees, to deepen the channels of communication with other parties participating in the exercise, and to work together to rehearse and improve the implementation of crisis management procedures.

One scenario that has received a lot of attention from several actors in recent years is the "large-scale, prolonged power outage" (→ Chapter 2.4.5). In Germany, there is no one body with responsibility for emergency planning for power outages. Instead, a number of state actors working at the federal, regional and community levels and critical infrastructure operators, each implementing measures within their own fields of responsibility. The "Emergency Power Framework Concept" (Rahmenkonzept Notstrom) has been created to take a bird's eye view of this mix of measures, to record the state of knowledge on an ongoing basis, to develop tools, and to identify gaps in planning and information when it comes to emergency planning for power outages (→ Infoboxes 18, 19, 20 and 21).

2.4.1 A collective national task: cooperation between the federal and regional governments

The CIP Strategy (BMI 2009), passed by the federal cabinet, is aimed at actors at the federal level and outlines the strategic focus of the federal government. This strategic outline entails viewing critical infrastructure protection as a collective national task that requires close cooperation across administrative levels: operators of infrastructure are addressed by both federal and regional regulations, supervisory duties fall at various levels, large-scale failures demand cross-level crisis management and, lastly, civil protection responsibilities are shared between the federal and regional governments. It is for this reason that the CIP Strategy describes cooperation between the authorities at different levels as a key requirement for implementing its objectives. The importance of intense collaboration, discussion, and sharing of information between and amongst all actors involved is highlighted in conjunction with the strategy's cooperative approach (→ Chapter 1.2). Federal and regional authorities play a central role here; setting up suitable structures is cited as a tangible step in the implementation process.

At the time the CIP Strategy was adopted, critical infrastructure protection was also anchored in the updating of the "Internal Security Programme" at the Standing Conference of State Interior Ministers and Senators (IMK) in 2008/2009 (cf. IMK 2009). Critical infrastructure protection became established as a field of action and an intensifying of cooperation across all state levels was deemed essential. The programme states that the federal and regional governments, while retaining their responsibilities, will strive to create interdepartmental structures and establish coordinating bodies for this purpose. Prior to this, the IMK's working group AK V – responsible for the fire service, rescue forces, disaster management and civil defence – had commissioned an inter-state working group to draw up recommendations for cooperation at the federal and regional levels in the field of critical infrastructure protection.

The recommendations included providing a structure for sharing knowledge by means of regular meetings. These meetings have been taking place between the federal and regional interior departments since 2012 and have become established as a platform for confidential exchanges between all those involved as well as a forum for discussions about issues concerning critical infrastructure protection across all levels. From 2020, the critical infrastructure protection liaison office's informal working group has been in operation at the federal and regional levels.

2.4.2 UP KRITIS – the collaborative platform for federal authorities and operators

UP KRITIS

Operators of critical infrastructures can be both public and private bodies. The vast majority of critical infrastructures are, however, operated by private companies. With this in mind, the CIP Strategy lists "trusting cooperation between the state and business and industry" (BMI 2009, p. 10) as one of its guiding principles. In terms of the institutional structure, this can be seen in UP KRITIS – a platform for public and private sector cooperation between operators of critical infrastructure systems, their associations, and the responsible state bodies.

The origins of UP KRITIS date to 2007, when the "CIP Implementation Plan" (BMI 2007a) was submitted to the "National Plan for Information Infrastructure Protection" (BMI 2005b), which had been passed two years previously. This was a response by the federal government to the ever-increasing economic and societal importance of IT systems and to the growing presence of threats facing these systems. The CIP Implementation Plan was drawn up by the federal government in collaboration with operators of critical infrastructures. It also served to institutionalise the cooperation between these actors in the field of critical infrastructure protection as "UP KRITIS" over the course of its implementation, beginning with IT security questions.

Up until 2013, UP KRITIS organised cooperation between operators of critical infrastructures and the federal authorities tasked with critical infrastructure protection in four working groups. Work focused on the areas of emergency response and crisis exercises, as well as crisis reactions, and crisis management, which had been outlined in the roadmap for the CIP Implementation Plan. In order to intensify discussions on cross-sectoral issues, the working groups met at regular plenary sessions. In addition to two published recommendations (UP KRITIS 2008a; UP KRITIS 2008b; latest versions: UP KRITIS 2014b; UP KRITIS 2014c), this collaboration also resulted in internal studies, for example on IT dependencies, and some public papers (see https://www.upkritis.de for download).

In 2011, it was decided that the cooperation was to be restructured in order to be able to better deal with the challenges of digitalisation and the rise in cyber threats and their increasingly sophisticated nature, as well as to meet the needs of the increasing number of participants. The intention was not just to build on inspiration from the CIP Strategy and the Cyber Security Strategy (BMI 2011b; → Infobox 7) but also, by way of this strategic restructuring, to reach out to as many different organisations as possible from the field of critical infrastructure protection. Considering "physical protection" and IT security aspects separately had proven to be insufficient; a focus was therefore placed on an integrated approach based on the use of IT in critical processes. In February 2014, the UP KRITIS plenary passed its new basic principles and objectives (UP KRITIS 2014a), agreeing on a new structure and a new topical focus. Since then, "UP KRITIS" has been the standalone name and is no longer just the acronym within the CIP Implementation Plan.

Collaboration in UP KRITIS includes tactical and operational components based on a tried and tested model from an early phase of UP KRITIS. Here, the focus is on establishing a constant sharing of information about cyber security incidents, anomalies, and the current IT threat level between participants as part of a defined communications structure. Information provided by operators is passed on to the BSI for analysis (either directly or via a single point of contact within the industry). The BSI collates, analyses, and evaluates the information it receives, combines it with information from other sources and then makes it available in the form of status reports, reports, and (early) warnings. In order to ensure that the (sometimes highly sensitive) information can be shared, clear rules are required in addition to a suitably secure technical platform. These rules include a "traffic light protocol" to differentiate between different levels of confidentiality (cf. 2017b).

A related aspect is the strategic cooperation in committees set up to discuss conceptual issues, in particular the branch working groups (BAK) and the topic working groups (TAK). In the BAKs, operators from a specific industry come together with the responsible authorities within this branch. For example, the BAKs play a key role in compiling "industry-specific security standards" (B3S) for the legally compliant implementation of requirements stemming from the *IT Security Law* (→ Chapter 2.2.1 and Infobox 16). The TAKs, which by their nature are temporary bodies, look at topics that go beyond the scope of individual industries, such as the security of industrial control systems, supplier and manufacturer requirements, cross-sectoral recommendations on how to prepare for a crisis and organising exercises.

Spokespersons from the BAKs and TAKs, members of UP KRITIS, which coordinates the work between the plenary sessions, and the offices staffed by BSI personnel all take part in the plenary sessions. UP KRITIS is advised by a Council. This is made up of representatives from the sectors involved in UP KRITIS, as well as the BMI, BSI and BBK. The Council makes suggestions regarding UP KRITIS's strategic objectives and projects. The council representatives from private industry make up the Economic Advisory Council. The BAKs and TAKs focus on IT security issues, although they no longer deal exclusively with these topics; so-called "physical protection" against other threats from the All-Hazards Approach is now also addressed (→ Chapter 1.2).

The cooperation in UP KRITIS has developed into a model for success and has been met with growing interest by an increasing number of participants over time. Particularly since the *IT Security Law* was passed, there has been a steady flow of companies from the CI sectors (→ Infobox 2), although not all of these are looking to actively participate in the working groups. The new structure, which differentiates between "participants" and "members", has proven its worth in this respect: in principle, any company belonging to one of the sectors can participate in UP KRITIS. Representatives from a company that plays an active role in the UP KRITIS committees are members of UP KRITIS and have the right to vote in the respective committees. In addition to operators, regulatory bodies such as the Federal Financial Supervisory Authority (BaFin) and the Federal Network Agency (BNetzA) participate in UP KRITIS. In order to intensify and perpetuate exchange of know-how at the federal and regional levels in cooperation with operators, the German federal states have also been represented in UP KRITIS committees since the end of 2014.

Since 2017, UP KRITIS has had a mandate – a political voice – expressed through the Economic Advisory Council. It can now be involved and consulted, for example in the context of regulatory projects on cross-sectoral issues, without anticipating the sector-specific consultation of associations laid down in Section 47 of the *Joint Rules of Procedure of the Federal Ministries* (GGO 2011). On the other hand, it is now easier for UP KRITIS to make the concerns of operators known to public bodies.

As of December 2019, 670 companies and authorities have been registered as participants of UP KRITIS; there are currently 14 BAKs and 11 TAKs active.

Infobox 16: "Cooperative lawmaking" – implementing the IT Security Law

The *IT Security Law* saw the cooperative approach that had been established within critical infrastructure protection be transferred into a legislative process (→ Chapter 1.2). The specialist expertise of the operators was not only applied in consultations for drafting the legislation, it was also included in other stages in the process. As a collaborative platform between authorities and operators, UP KRITIS played a key role in this (→ Chapter 2.4.2).

The IT Security Law applies "where a modern society can least afford failures: in the IT systems of critical infrastructures" (BSI 2017a, p. 13). As an omnibus act, it altered and supplemented a range of existing laws, including the *Act on the Federal Office* for Information Security (BSIG).

Operators of critical infrastructures, as defined in Section 2(10) BSIG, must adhere to a minimum level of IT security and report significant IT interruptions to the BSI. When it came to implementing the *IT Security Law,* UP KRITIS acted as a link between state authorities and operators of critical infrastructures during (at least) two key stages.

One concerned the question of which specific "facilities, equipment or parts thereof" (Section 2(10) BSIG) were to be viewed as critical infrastructures within the context of the BSIG. To this end, the law provides for the instrument of a statutory order and sets out a number of requirements for its implementation in Section 10(1) of the BSIG: critical infrastructures are to be identified as those involved in providing "services to be considered critical" within the sectors addressed by law with "a degree of supply to be considered important". The "degree of supply to be considered important" is to be determined by means of industry-specific threshold values. So-called "core teams" were formed to transform these specifications into a regulation that could be accurately implemented within the industries in question. The core teams consisted of representatives from the BSI, BMI, BBK, the responsible federal departments, and operators of critical infrastructures or their associations. The BAKs working within UP KRITIS were the first port of call when it came to finding suitable contacts for the core teams. The *BSI Critical Infrastructure Ordinance* was eventually passed in two rounds in 2016 and 2017 (cf. Figure 17) and allows operators to check whether their "facilities, equipment or parts thereof" are "critical in the sense of the law" (cf. Figure 18).

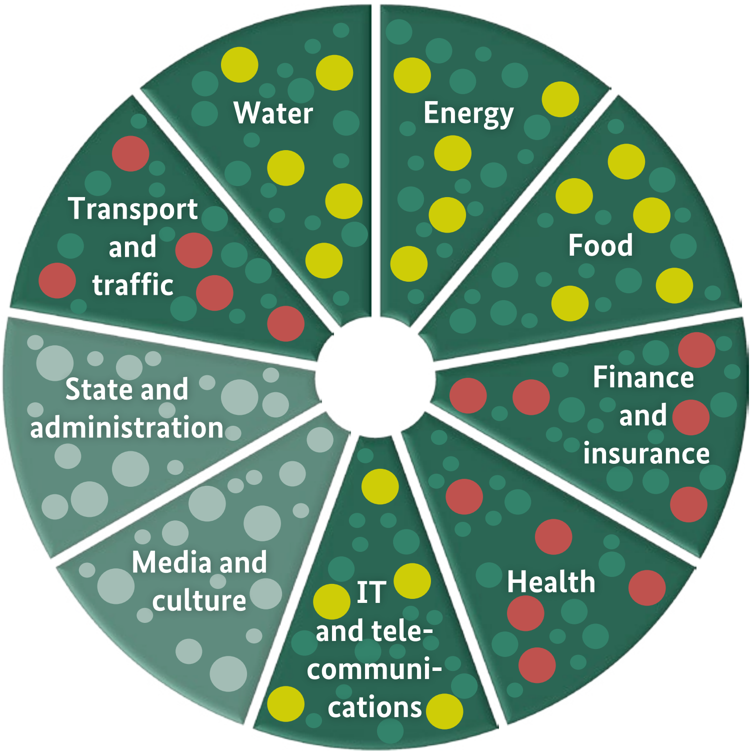


Figure 17: The *BSI Critical Infrastructure Ordinance* regulates which particular infrastructures are seen as "critical" within the sectors addressed by the *IT Security Law* (dark green). The ordinance was developed in two stages: 2016 (yellow dots) and 2017 (red dots) (source: modified in accordance with BSI 2017a, critical infrastructure protection from the IT Security Law and UP KRITIS, p. 17, translated by: BBK).

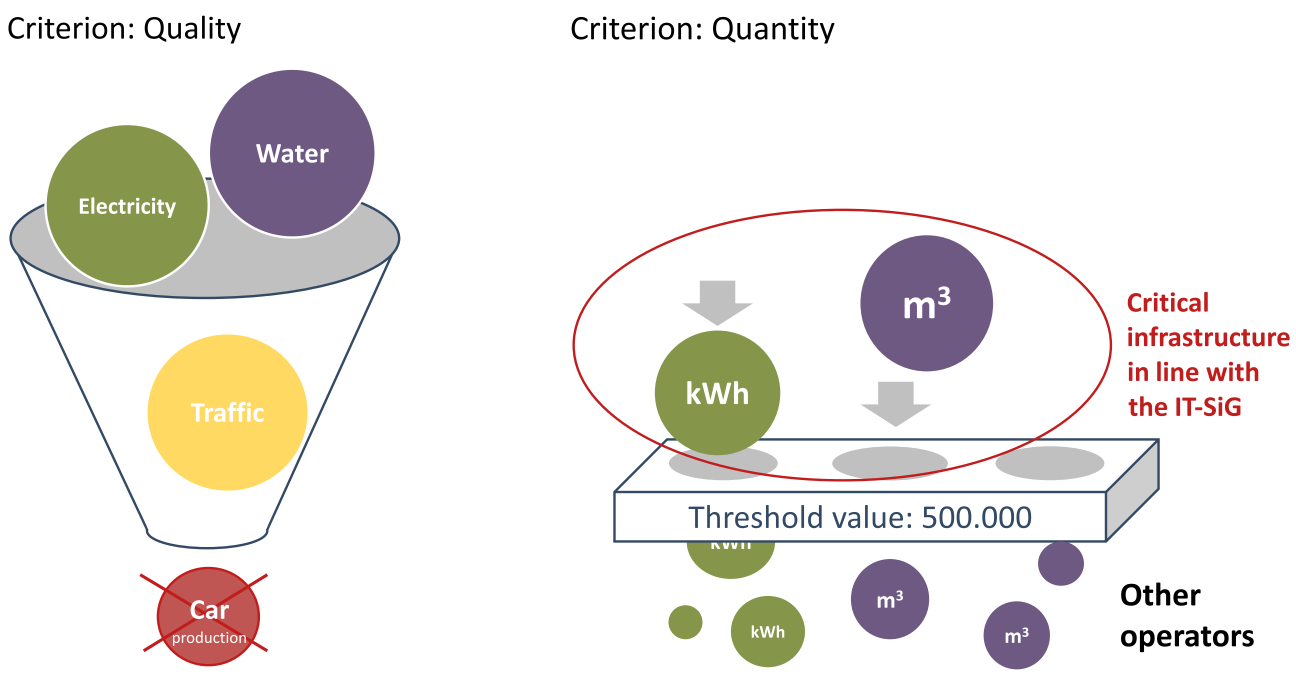


Figure 18: In order to determine which plants and facilities are classed as critical infrastructures within the context of the *IT Security Law*, the *BSI Critical Infrastructure Ordinance* applied a combination of qualitative and quantitative criteria: affiliation to one of the addressed sectors on the one hand, and the degree of supply considered to exceed the relevant threshold on the other values (source: according to BSI, translated by: BBK).

UP KRITIS played another key role in substantiating Section 8a (1) BSIG. According to this provision, operators of facilities deemed to be critical infrastructures by the *BSI Critical Infrastructure Ordinance* are obliged to ensure that the information technology they use for their critical services meets the “latest state of technology”. The law gives operators and industry associations the option of describing the state of technology through “industry-specific security standards” (B3S) (cf. Section 8a(2) BSIG). Thus it has been possible to provide an accurate standard to describe the “state of technology” that is compliant with the law for specific industries (→ Chapter 2.2.2).

The particular constellation of actors here meant that the UP KRITIS BAK groups offered an ideal environment in which to develop B3S: most of the B3S that have since been presented were either drawn up directly in the BAKs or in close cooperation with them. Furthermore, the involvement of UP KRITIS’s structures made it far easier to facilitate knowledge-sharing between industries – so there was no need to reinvent the wheel in cases where similar problems needed to be solved for multiple industries. Upon request, all proposed B3S are reviewed by the BSI in cooperation with the BBK and, if necessary, with the involvement of supervisory authorities and, if these measures are deemed suitable, approved. The approved B3S can be used as a basis for the proof that must be provided to the BSI every two years that the IT security requirements set out in the BSIG are being adhered to (cf. Section 8a(3) BSIG).

Even though the B3S are predominantly aimed at operators of critical infrastructures as defined in the *BSI Critical Infrastructure Ordinance*, they also provide a guide for the level of IT security required based on the current state of technology for *all other* operators in the corresponding industries. Hence they also have an effect beyond the regulatory scope of the BSIG and can contribute to critical infrastructure protection as a result.

2.4.3 Integrated risk management – systematically bringing actors together

Risk and crisis management for critical infrastructures does not just depend on the preparations made by each individual actor – cooperation is also key. For example, a power outage (→ Chapter 2.4.5) will be dealt with most effectively when network operators and civil protection bodies have already discussed in advance the possible actions they can take.

Collaboration between civil protection actors and the often privately run operators is a crucial factor for successful risk mitigation and crisis management in critical infrastructure protection. But evidence suggests there is room for improvement: in many cases, each individual organisation draws up their own risk management plan and works with their own threat scenario. When they reach the limits of their own potential, they often assume that a third party – such as the fire service, the Federal Agency for Technical Relief or the police – will intervene. But in the event of a more serious incident occurring, these actors would not be available everywhere at the same time. This is why part of the focus of critical infrastructure protection is on an "integrated risk management" that brings together state and private entities in all stages of risk management (cf. Figure 19). Rather than focusing on each actor's individual point of view, the perspective should be shifted to an integrated viewpoint and the focus moved to the organisational links and sharing of information, expertise and results between relevant actors. This approach is being put into practice more and more often after it led to advances in risk management within specific facilities. The realisation that collaboration is necessary is becoming increasingly prevalent and is leading to steps being taken towards joint risk management by both state and private bodies. Groundwork for the development and rehearsal of integrated risk management has been laid as part of the research project "CIRMin" (→ Infobox 17). The procedure has already been successfully applied in certain contexts. The thinking behind this procedure also stems from the cooperation under the aegis of UP KRITIS (→ Chapter 2.4.2) as

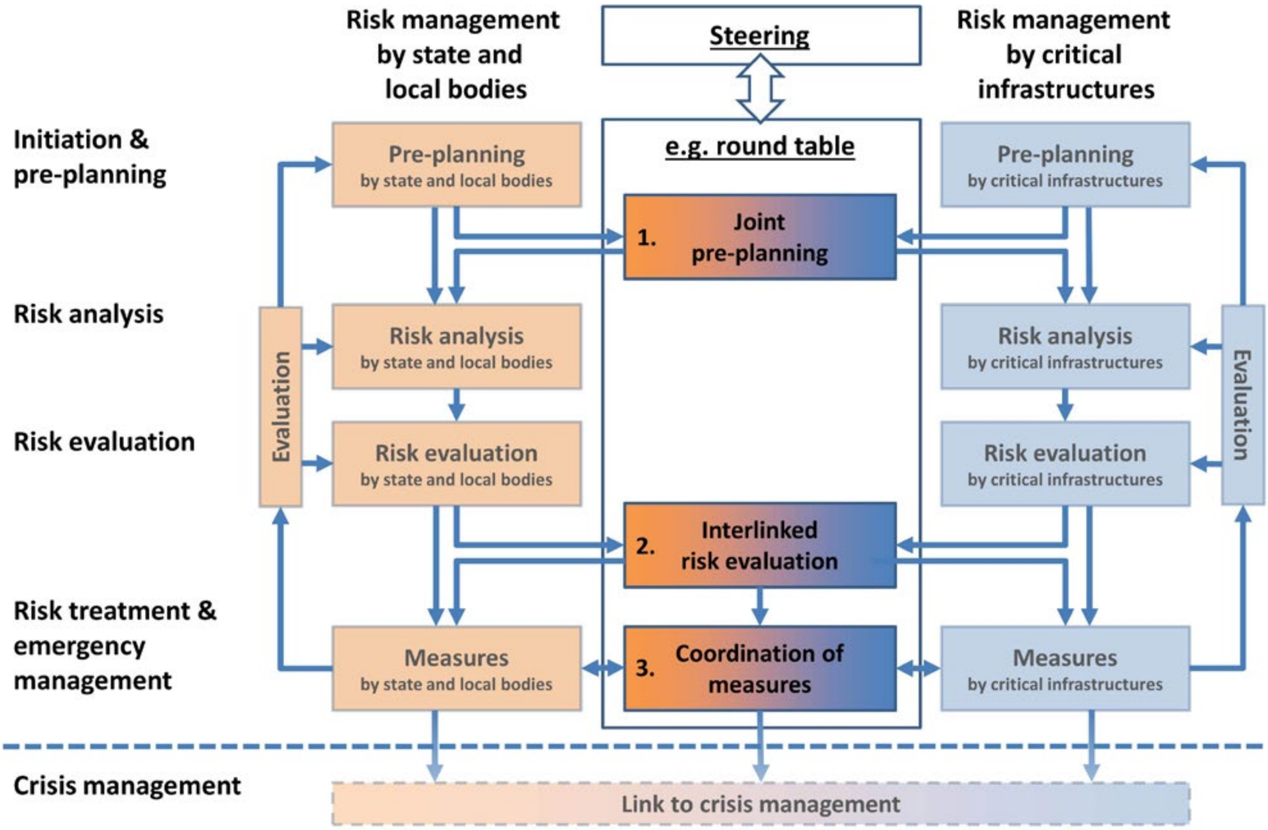

Risk management by state and local bodies
Steering
Risk management by critical infrastructures
e.g. round table
Initiation & pre-planning
Risk analysis
Risk evaluation
Risk treatment & emergency management
Crisis management
Pre-planning by state and local bodies
Risk analysis by state and local bodies
Risk evaluation by state and local bodies
Measures by state and local bodies
Evaluation
1. Joint pre-planning
2. Interlinked risk evaluation
3. Coordination of measures
Pre-planning by critical infrastructures
Risk analysis by critical infrastructures
Risk evaluation by critical infrastructures
Measures by critical infrastructures
Evaluation
Link to crisis management

Figure 19: Processes in integrated risk management (source: DIN SPEC 91390:2019-12, p. 9, translated by: BBK, permission by DIN e. V.).

well as other types of collaboration. To establish integrated risk management across all levels, the procedure is taught in seminars at the BBK's Academy for Crisis Management, Emergency Planning and Civil Protection (AKNZ) and on other sites, and has been discussed and presented in lectures and publications (cf. BBK 2018a). This helps actors to be better prepared where integrated risk management is practised – and, in the future, this should be everywhere.

Infobox 17: Research on integrated risk management – the CIRMin project

The research project "Critical Infrastructures – Resilience as a Minimum Supply Concept" (CIRMin) was funded by the security research programme known as "Civil Security – Increasing Resilience in the Case of Crises and Catastrophes" (→ Chapter 2.3.3). The project investigated the dependencies between different critical infrastructures in Germany. The vulnerability of the water supply in the case of an extensive and sustained power cut was analysed in particular detail. The findings were used to draw up a concept for the minimum supplies required by the populace during a power cut. The project brochure entitled "Steps to a Minimum Supply Concept. Critical Infrastructures and Resilience" (cf. Fekete et al. 2019) provides insights into other findings from the project.

One of the project's priorities lay in bringing together different actors – including representatives from operators of infrastructure, disaster management, the scientific community, and the general population – in a wide-ranging dialogue to formulate accurate insights and practical measures for a minimum supply concept. The "integrated risk management" procedure has played a special role here, seeking to systematically connect the risk management of state actors with the risk management of operators of critical infrastructures. The CIRMin project enabled the procedure to be developed further and led to the DIN specification on "Integrated Risk Management in Civil Protection" (DIN SPEC 91390:2019-12; → Chapter 2.2.2). It names the interfaces for the various risk management processes and highlights the potential of a structured sharing of information between the parties involved. As a DIN SPEC, it is neither a norm nor a piece of legislation, so it is itself neither binding nor obligatory. Despite this, it has been possible to introduce a structured discussion that has shone a spotlight on the issue and which could lead to the development of a genuine standardardisation of procedures in the future. The CIRMin project also resulted in tools being developed, intended to support the implementation of integrated risk management, particularly at a local level. These tools were then further developed in collaboration with project partners and were put into practice in the project's pilot regions of Cologne, Mülheim an der Ruhr, Kerpen, and the Rhein-Erft-Kreis district.

2.4.4 Strategic crisis management exercise LÜKEX – never without CI!

LÜKEX
INTERSTATE AND INTERMINISTERIAL CRISIS MANAGEMENT EXERCISE

Identifying challenges, progressing together, learning from one another – these lie at the heart of the German Interstate and Interministerial Crisis Management Exercise series known as LÜKEX. Since 2004, the German Interstate and Interministerial Crisis Management Exercise (in German: **L**änder- und Ressort**ü**bergreifende **K**risenmanagementübung (**Ex**ercise)) has been taking place under the acronym LÜKEX, and operators of critical infrastructures are always involved. Over the past 16 years, it has been possible to involve companies from all CI sectors (→ Infobox 2) within the LÜKEX working groups and to address extraordinary crisis scenarios by working together in teams. Scenarios are always chosen on the basis that they affect large parts of society. Previous LÜKEX exercises have addressed cyber attacks, power outages, storm surges, and gas shortages (cf. Figure 20). Networks are established in the run-up to each LÜKEX, which usually take place every two years. Problems and questions are addressed confidentially and are ideally used to establish a solution in advance of the two main days set aside for the exercise to take place. Operators of critical infrastructures play a key role and actively shape the simulated scenario at the regional level, or in the central project group at the federal level. The networks established as a result of this remain in place even after the exercise has been completed, and contacts that are made can be used in the event of real-life situations occurring.

The exercise's objective is better preparation for comparable incidents, e.g. thanks to specially trained employees, tried and tested channels of communication with other actors involved in the exercise and procedures that have been tested together. The LÜKEX scenarios are designed so that the different actors have to work together: the fictitious crises can only be overcome if a joint strategy is put into practice.

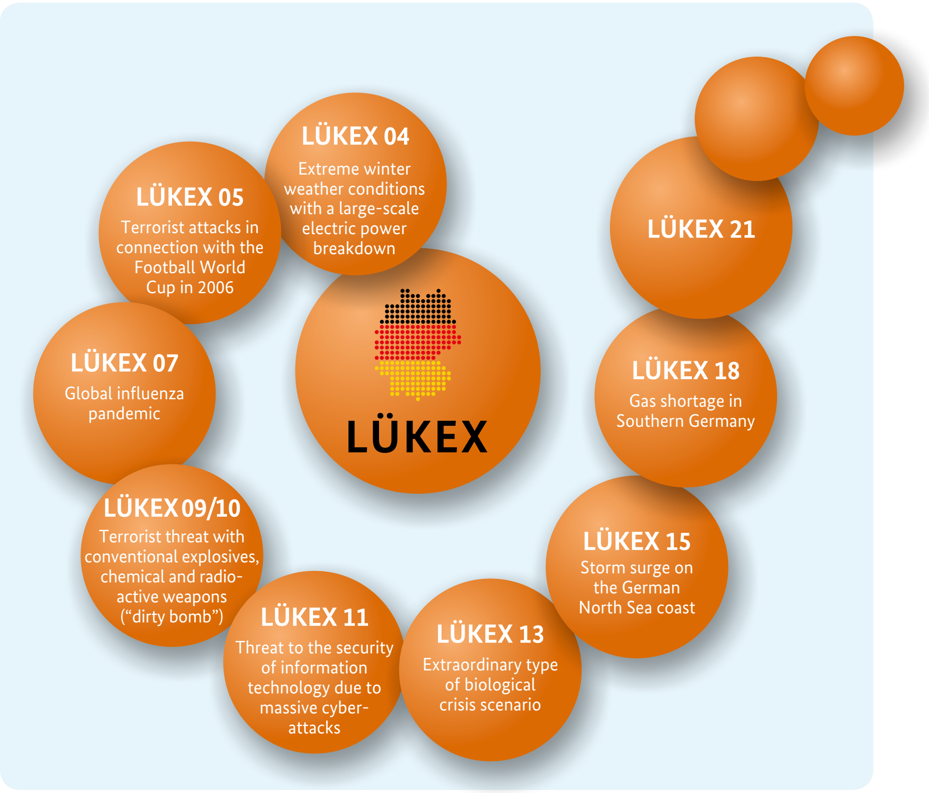

LÜKEX
LÜKEX 04
Extreme winter weather conditions with a large-scale electric power breakdown
LÜKEX 05
Terrorist attacks in connection with the Football World Cup in 2006
LÜKEX 07
Global influenza pandemic
LÜKEX 09/10
Terrorist threat with conventional explosives, chemical and radio-active weapons ("dirty bomb")
LÜKEX 11
Threat to the security of information technology due to massive cyber-attacks
LÜKEX 13
Extraordinary type of biological crisis scenario
LÜKEX 15
Storm surge on the German North Sea coast
LÜKEX 18
Gas shortage in Southern Germany
LÜKEX 21

Figure 20: An overview of the exercises carried out to date as part of the German Interstate and Interministerial Crisis Management Exercise (LÜKEX) (source: BBK, translated by: BBK).

Without the active involvement of companies, it would not be possible to offer a realistic representation of many of the relevant processes, and the knowledge gained would be considerably reduced. One example of this is the complex reporting and information channels that would be relevant in the case of a gas shortage, as came to light during the LÜKEX 18 scenario (cf. BBK 2019b). This type of exercise could only be implemented thanks to the involvement of genuine gas suppliers. When it comes to LÜKEX, public authorities benefit from the involvement of private industry, while companies also need the state authorities to be able to improve co-operation in the event of crises.

Theme days are organised as part of the preparations for the exercise. These specialist events give participants the chance to approach issues from a different perspective. Those planning the exercise and many of the interested parties also gain a deeper understanding of the specialist world of the respective exercise topic. A conference transcript is produced for each theme day, featuring the presentations given by expert speakers. In order to record the findings from each LÜKEX over the long term, each exercise concludes with a joint progress report. The exercise participants take up the recommendations for action formulated in the progress report and are responsible for implementing these themselves and in cooperation with others, if necessary. Associations act as multipliers to disseminate the findings within their respective branches.

Operators of critical infrastructures have been playing an active role in preparing, implementing, and evaluating these strategic crisis management exercises for over 16 years. The LÜKEX series of exercises will continue to facilitate and enhance cooperation between operators and public authorities in the field of crisis management in the future. After all, without CI operators there would be no LÜKEX! The BBK provides information about the series of exercises known as LÜKEX, as well as the aforementioned conference transcript and evaluation reports (www.luekex.de).

2.4.5 Planning for the blackout together: the framework concept for crisis management

Over recent years, a number of state and regional actors, as well as private companies, have grappled with the issue of a power outage occurring. The quality of the electricity supply in Germany is exceptionally high; the country hasn't experienced large-scale, long-lasting power cuts until now. However, should this occur, it would impact all aspects of life, including communication, healthcare, mobility, and food supply. The Office of Technology Assessment at the German Bundestag (TAB) has looked into the scenario of a large-scale power cut lasting several weeks and described the consequences of such an event in detail in a 2010 report (cf. BT-Drs. 17/5672). The report came to the following conclusion: "Although the probability of a prolonged power blackout affecting several federal states may be low, if such an incident did occur, the resulting consequences would be tantamount to a national disaster" (BT-Drs. 17/5672, p. 15).

In Germany, there is no *one* body with responsibility for emergency planning for power outages. State actors at the federal, regional and local levels, and CI operators implement their own measures. These include a range of activities, such as drawing up and executing contingency plans, procuring emergency generators or participating in working groups and exercises concerning power outage scenarios. The sheer number and diverse range of measures taken by the various actors at different levels and with the involvement of several departments can lead to gaps in planning and information, which cannot be identified by the individual parties from their own perspective and which are instead only evident when viewed "from above". As a result, during the development of the "Emergency Power Framework Concept", the BBK compiled regular reports on the state of knowledge and drew up recommendations to show how gaps in planning and information in the field of crisis management for a power outage can be resolved – both by and between the actors. Gaps in planning can, for example, occur when calculating required capacity, when setting priorities or when stipulating various kinds of targets and threshold values. At the same time, these are the precise points at which action can be taken: for example, when it comes to maintaining an emergency electricity supply without the need to refuel, the BBK recommends a standard ideal target of at least 72 hours for all critical infrastructures. This objective has since become established within the expert community (→ Infobox 18). In some areas of responsibility, the transport of fuel from fuel depots and its targeted distribution to end users has emerged as a significant gap in contingency planning for power outages (→ Infobox 20).

In recent years, measures have been developed and implemented across all levels in Germany in order to improve crisis management for power outages. The main challenge remains the need for discussion and cooperation between actors, as responsibilities are spread horizontally (across different departments) and vertically (across federal levels).

Infobox 18: Emergency power supply for operators and authorities

The problem of providing sufficient emergency power for CI operators and authorities has been known since the 2004 LÜKEX on power outages (→ Chapter 2.4.4). Binding regulations that apply across Germany have only been passed for a very few sectors, like hospitals. Where these are in place, they often only concern a limited number of sectors and cover varying time frames. As a result, the BBK has drawn up recommendations on how facilities can calculate their own energy requirements and establish and safeguard an emergency power supply (cf. BBK 2015a). These recommendations are the result of a continuous development process that incorporates the experiences of an array of actors with whom the BBK has worked together on the issue of emergency planning in recent years. The recommendations also include a reference value of at least 72 hours for the stockpiling of fuel to facilitate harmonisation within emergency planning. The reference value is derived from the fact that 72 hours is expected to be sufficient to guarantee further provision with fuel in the case of a long-lasting power cut. The target of 72 hours was then adopted in many other sectors, for instance in the “Code of Practice for Maintaining a Secure Gas Supply in the Event of a Failure of Regular Communication” by the German Technical and Scientific Association for Gas and Water (cf. DVGW G 1003; → Chapter 2.2.2). Recommendations have also been compiled for the storage of fuel. If diesel fuel is stored for long periods without being used, there is a risk of microbiological contamination. To address this contingency, effective measures must be taken, as fuel has to be in perfect condition to be of use during an emergency power situation.

Infobox 19: Deployment during a power outage – the capabilities of the Federal Agency for Technical Relief

The Federal Agency for Technical Relief (THW) is Germany’s operational deployment organisation and provides technical assistance in accordance with the Federal Civil Protection and Disaster Assistance Act. Based on the provisions of the THW Law, the services of the THW can be requested by the authorities responsible for hazard prevention in the event of large-scale emergencies, including when the situation concerns the provision of emergency power (cf. THW 2014). The THW provides support but does not take over the remit of the responsible bodies.

The “THW Framework Concept” provides the basis for developing and extending the THW’s capabilities in the field of crisis management, as well as in other spheres of activity, and provides for various capabilities within the area of emergency power supply. To guarantee the operational capability of the THW or other deployment organisations, emergency power capacities of 13 to 50 kVA are to be provided. The THW has enhanced this capability with the specialist group “Emergency Supply and Repair” and has introduced it nationwide. In the future, each local THW association will have this capability. A different order of magnitude is required for the provision of emergency power to supply larger deployment sites or staging areas in isolated operations. Emergency power capacities of 175 to 200 kVA are provided for these purposes. The THW Framework Concept provides for enhanced capabilities for the responsible specialist group “Electrical Supply”. The THW is aiming for this expansion to enable it to more effectively help to supply individual parts of the network or to support networks with partial outages.

Figure 21: The THW’s emergency power capacities in deployment (source: THW).

Infobox 20: Fuel supply in the case of a power cut

Emergency vehicles and emergency generators require a diesel fuel supply in case of an incident. As such, the supply of fuel is a fundamental challenge when it comes to dealing with a long-lasting and large-scale power outage. In a first effort, stakeholders from the regional states, local authorities, and the petroleum industry came together under the coordination of the BBK to address the outsourcing and distribution of fuel in the event of a power outage. Their results were summarised in a recommendation (BBK 2017). The solutions span from stipulating petrol stations and fuel depots supplied with emergency power, to prioritising those who are entitled to fuel in advance, to organising transport capacities, to regular exercises involving relevant actors. Further coordination between the federal and state governments on legal issues, responsibilities, planning, and organisation is urgently required and will be taking place in the form of a working group convened by the Federal Ministry for Economic Affairs and Energy (BMWi), which is in charge of the project.

Figure 22: (Source: Skitterphoto / pixabay)

Infobox 21: What should I do in the event of a power cut? Information for citizens about power outages

It is not just important for the authorities and CI operators to be well-positioned to deal with a power outage – citizens need to be prepared, too. This is especially relevant for those who depend on the electricity supply more than others, such as patients on ventilators or caregivers needing to prepare baby food. But many people also require other supply services that can no longer be guaranteed in the case of a power outage. Anyone who receives meals on wheels or uses care services needs to consider the issue. At the end of the day, it is up to each and every individual to provide for themselves and for the people around them.

Figure 23: (Source: Mark Evans / E+ / Getty Images)

The BBK provides information in the form of a brochure (BBK 2019c) and a video (BBK 2015b), to help support people in preparing for power outages. While emergency provisions should always include an emergency supply of water and food, and it is always recommended to have a supportive network of people within the community, setting up your own emergency power supply should be carefully considered. The options for this have been investigated in detail in a research project on a self-sufficient emergency power supply for the general public (cf. BBK 2018b). Instructions for setting up and managing your own emergency power supply are provided in the aforementioned brochure and in this video (BBK 2015c).

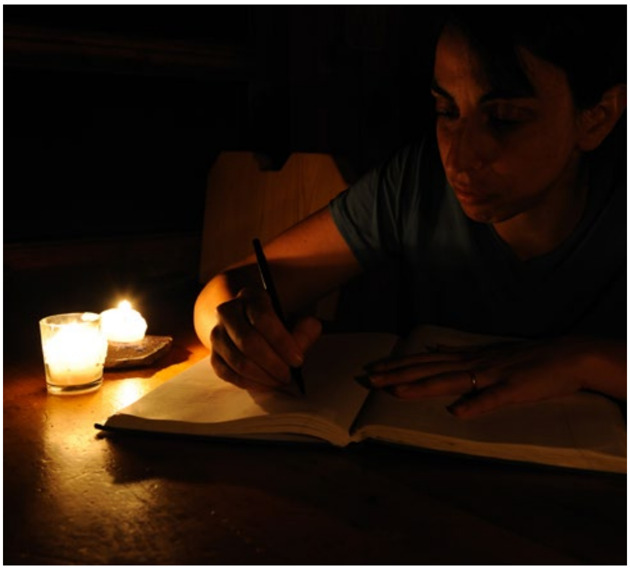
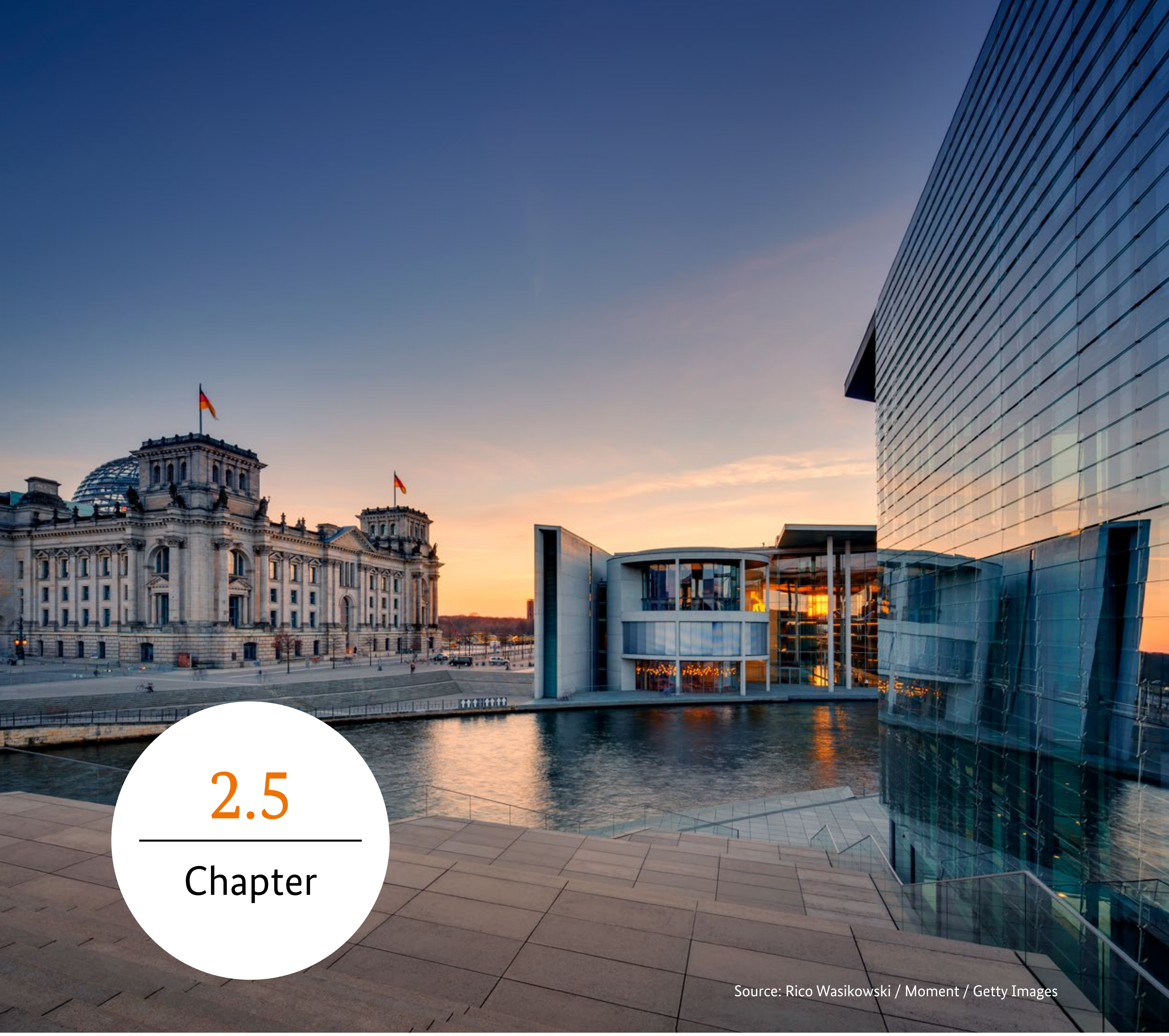


Figure 24: (Source: Ashok Rodrigues / E+ / Getty Images)



2.5

Chapter

Source: Rico Wasikowski / Moment / Getty Images

Critical infrastructure protection as a sectoral task

When it comes to critical infrastructure protection, much importance is given to accommodating cross-sector connections and interdependencies. However, the fact that many approaches and activities within this field have a single-sector focus (→ Infobox 2) does not contradict this. Rather, there is a need to substantiate overarching approaches for different sectoral contexts and to address fundamental issues in a sector-specific manner. As such, many methods have been tailored within sectors, branches and even specific types of facilities, and sectoral networks relating to critical infrastructure protection have also become established independently of UP KRITIS.

In 2006 and following a number of fatal incidents, including the fire at the Duchess Anna Amalia Library (2004) and the flooding of the River Elbe (2002), work began on the “Guidelines for the protection of cultural property” (SiLK), initiated by the German Conference of National Cultural Institutions (KNK). This web-based advice and evaluation tool covers topics concerning the protection of cultural property and is aimed at museums, libraries, and archives as operators of important facilities within the CI sector *media and culture* (→ Chapter 2.5.1).

In order to sensitise and support operators and authorities working in the *water* sector, the BBK has published two recommendations on the security of the potable water supply (→ Chapter 2.5.2). The first part supports bodies responsible for the water supply in communities in investigating and assessing risks, particularly in conjunction with extraordinary threat levels. The second part describes the steps required to develop emergency planning.

The circulars issued by the Federal Financial Supervisory Authority (BaFin) play a central role in shaping risk management in the *finance and insurance* sector. They define the minimum requirements for risk management in the banking and financial services sector and specify IT security aspects for operators of critical infrastructures in the banking, insurance, and capital management supervisory sectors (→ Chapter 2.5.3).

As to critical infrastructures in the *health* sector, methodological principles on risk and crisis management have been provided in various publications and tailored to the specific needs of hospitals. With the help of experts and partners, a guide for risk management in hospitals was published in 2008. Meanwhile, a guide published in 2013 addressed IT security issues in hospitals. The handbook on alert and deployment planning for hospitals will detail planning measures that can be used to maintain the capacity and functioning of hospitals in damaging situations (→ Chapter 2.5.4).

The BMVI Network of Experts brings together the expertise and know-how of seven departmental research institutes and specialist authorities in the business division of the Federal Ministry of Transport and Digital Infrastructure (BMVI) and also addresses questions concerning critical infrastructure protection in the *transport and traffic* sector. The current and expected future effects of climate-related extreme events on different modes of transport are being investigated in various thematic areas, with options for adaptation currently being developed (→ Chapter 2.5.5).

2.5.1 The “Guidelines for the protection of cultural property”

SiLK
SicherheitsLeitfaden
Kulturgut

The *Convention for the Protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention 1954* (referred to in this report as the Hague Convention) aims to protect cultural property from destruction, theft, and plunder during armed conflicts and to prevent cultural items being used as pawns in psychological warfare (→ Infobox 3). Germany has ratified both the treaty and its two supplementary protocols, and has tasked the BMI with ensuring its obligations are met (cf. *Law on the Convention of 14th May*

1954 for the Protection of Cultural Property in the Event of Armed Conflict from 11th April 1967). These duties are administered by the BBK and by the federal states on behalf of the federal government. Implementing the Hague Convention is part of the "Civil Defence Concept" (BMI 2016b, → Chapter 2.3.2) in Germany.

The "Guidelines for the protection of cultural property" (SiLK, KNK) – a web-based advice and evaluation tool for topics concerning the protection of cultural property – plays a key role in implementing the Hague Convention. The project was launched in 2006 by the Conference of National Cultural Institutions (KNK) in light of the destruction of cultural heritage by the fire at the Duchess Anna Amalia Library (2004) in Weimar and by the flooding of the River Elbe (2002). The contents of SiLK were compiled in cooperation with numerous experts and are updated regularly.

The tool features introductory texts, interactive questionnaires, and a pool of knowledge and serves to increase awareness with regard to security and protecting cultural property in museums, libraries, and archives as operators of important institutions within the CI *media and culture* sector (→ Infobox 2). SiLK assists staff in carrying out risk analyses and in evaluating the security status of their institution, points out deficits, and provides suggestions for possible steps that can be taken to guarantee the safeguarding and long-term preservation of our cultural heritage.

Recent developments include a concept for recovering cultural property in case of an armed conflict, which was presented in 2018 at the international SiLK expert conference "KULTUR!GUT!SCHÜTZEN!", which takes place every three years. In addition to drawing up the "Guidelines for the protection of cultural property", the SiLK team also runs workshops and seminars, and publishes, advises and reports on issues related to protecting cultural property.

SiLK had been funded by an arm of the Federal Ministry for Culture and the Media (BKM) since 2006, but the BBK took over its financing in 2016. More details about SiLK can be found on the KNK's website (www.konferenz-kultur.de).

Figure 25: (Source: Maik Schuck / Klassik Stiftung Weimar, Museen, A 1580)

2.5.2 Safeguarding the supply of drinking water – risk analysis and emergency planning

A reliable supply of drinking water is a vital foundation for society and the economy. In light of the exceptionally pressing need to guarantee security of supply, the constant availability of quality drinking water is considered a matter of course in Germany. Yet, it is also the result of comprehensive forward planning and continuous improvements to security measures. Extraordinary events have repeatedly pointed to the necessity of this approach. Thus, for example, it has become increasingly clear in recent years that, in addition to the new challenges to supply security posed by climate change, such as flooding, heavy rainfall, and droughts, cyber threats and terrorist or criminal threats could have such potential impacts on the water sector that companies and authorities need to include these possibilities in their risk assessments. To help raise awareness and support companies and authorities, the BBK has published two recommendations on the security of the potable water supply (cf. Figure 26).

“Part 1: Risk Analysis” (BBK 2019d) supports the bodies responsible for the water supply in communities in investigating and assessing risks resulting from natural hazards, technical failure, and human error, crime, terrorism, and warfare. The focus is on the structured analysis of risks and vulnerabilities in case of exceptionally damaging situations. “Part 2: Emergency Planning” (BBK 2019e) describes the steps required to draw up a plan for a replacement and emergency water supply. It includes becoming familiar with legal and organisational frameworks and identifying the additional resources deemed necessary, following analysis of the types of supply and resources available.

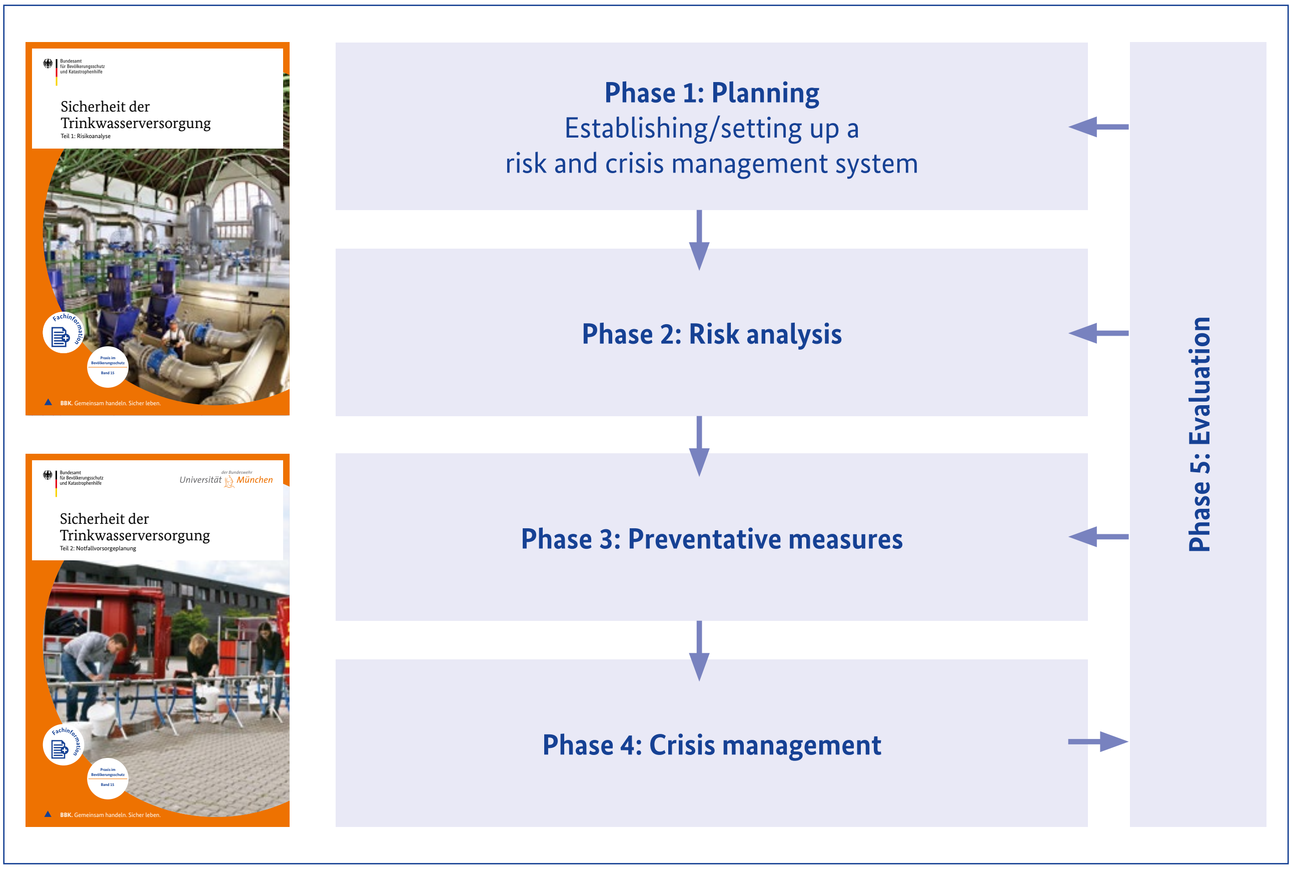

Sicherheit der Trinkwasserversorgung
Teil 1: Risikoanalyse
Sicherheit der Trinkwasserversorgung
Teil 2: Notfallvorsorgeplanung
Phase 1: Planning
Establishing/setting up a risk and crisis management system
Phase 2: Risk analysis
Phase 3: Preventative measures
Phase 4: Crisis management
Phase 5: Evaluation

Figure 26: Classifying the contents of “Security of the potable water supply” (BBK 2019d; BBK 2019e) in the context of the BMI’s risk and crisis management concept (→ Chapter 2.1.1; source: BBK, translated by: BBK).

In the spirit of integrated risk management, both recommendations aim for collaboration between all responsible parties working within the water industry, such as water suppliers, health authorities, and actors tasked with disaster management (→ Chapter 2.4.3). Numerous pilot projects have confirmed the practicality and feasibility of the risk analysis and emergency planning methods, which are recommended based on the generally acknowledged codes of practice (→ Chapter 2.2.2). The publications on the security of the potable water supply form the basis of the seminars taught at the BBK's Academy for Crisis Management, Emergency Planning and Civil Protection (AKNZ).

2.5.3 Requirements facing risk management and IT security in the finance and insurance sector

Risk management measures in the CI sector *finance and insurance* (→ Infobox 2) have been addressed by circulars issued by the Federal Financial Supervisory Authority (BaFin), which supervises banks and financial services providers, insurance undertakings, and securities trading companies in Germany. These circulars specify legal requirements for the entities being supervised and include the requirements that their IT systems and IT service providers must meet, which are in part related to critical infrastructure protection.

Examples include the circular on "Minimum Requirements for Risk Management" (MaRisk) in banking and financial services (Circular 09/2017, BaFin 2017). When considering possible applications, it is largely financial risks that spring to mind, and it is their management that the majority of the information provided in MaRisk relates to. However, the "Requirements for Risk Control and Controlling Processes" module also looks into so-called operational risks. According to Art. 4(52) of the *"Regulation on prudential requirements for credit institutions and investment firms"* (EU Regulation No. 575/2013), operational risk refers to the probability of losses occurring due to the inadequacy or failure of internal procedures, people or systems, or resulting from external conditions and events, including legal risks.

The institutes must guarantee that the relevant risks are identified and assessed each year, that incidents are recorded and their causes analysed, and that measures, which can also include disaster management measures, are implemented and monitored as part of risk controlling.

In 2017, BaFin published its circular "Supervisory Requirements for IT in Financial Institutions" (BAIT) in order to make transparent to institutions' managers the expectations of the banking supervisory authority concerning the secure design of IT systems and the requirements for IT governance (Circular 10/2017, latest version: BaFin 2018a). BAIT is the central pillar of IT supervisory requirements for the banking sector in Germany. In September 2018, in collaboration with the BSI and in order to make it easier to implement the requirements of Section 8a(3) BSI Act, BAIT was supplemented with a new module entitled "Critical Infrastructures" (cf. BaFin 2018b; → Chapter 2.2.1 and Infobox 16). This special module only applies to companies within the banking sector that are also classed as CI operators based upon the criteria listed in the *BSI Critical Infrastructure Ordinance*. As such, meeting the CI protection objectives – in this case ensuring basic provision of payment services to the population, including in a state of crisis – is a fundamental part of banking supervision.

In July 2018, the circular entitled "Supervisory Requirements for IT in Insurance Undertakings" (VAIT) came into force (Circular 10/2018, latest version: BaFin 2019a). Just as BAIT is for the banking sector, VAIT is a central component of IT supervision in the insurance sector. VAIT now also includes a module entitled "Critical Infrastructures", which applies to the respective insurance companies that are also classed as CI operators based on the criteria listed in the *BSI Critical Infrastructure Ordinance*. In October 2019, BaFin also published Circular 11/2019 "Supervisory Requirements for IT in German Asset Managers" (KAIT, BaFin 2019b).

2.5.4 Hospitals as critical infrastructure within the health sector

Hospitals are a vital feature in all our lives, especially in the event of serious incidents with large numbers of injured or ill people. A hospital unable to maintain its critical services can endanger the health and lives of its patients. The publications described below from 2008 and 2013, and those planned for 2020, all concern the hospital as critical infrastructure within the *health* sector (→ Infobox 2). Each of these reports feature methodological principles (→ Chapter 2.1) for use in hospitals that are tailored to the specific challenges facing this target sector. They are not unrelated; rather they have a specific bearing on one another. In addition, what these publications have in common is that they were produced by interdisciplinary working groups and project consortia rather than behind closed doors.

A comprehensive risk management system is vital for ensuring that hospitals are able to continue functioning even in crisis situations and to limit damaging consequences for patients, family members, and employees as much as possible. In 2008, the BBK published a guide entitled "Critical Infrastructure Protection: Risk Management in Hospitals" (BBK 2008) with the aim of using the methodological approach to establish a risk management system within hospitals. The guide stems from the work of a group comprising representatives from administration, professional associations, and hospital operators. The risk management procedure described in the guide provides instructions on how to identify critical processes within a hospital, to recognise their vulnerabilities to possible threats and to apply this information to draw up protection measures.

The "Guide to Risk Management in Hospitals" has been a key component of the series of guidelines on critical infrastructure protection for over ten years. An updated version is to be published in the near future.

Using these general approaches to risk management in hospitals as a basis, the guide on "Hospital IT Risk Analysis" (BSI 2013a) addresses the specific challenges arising from the use of information technology in hospitals. IT has become an essential part of hospital life and not just in the administrative area; patient medical care and general care are also largely supported by IT applications, including diagnostic measures, such as laboratory tests and imaging equipment.

But the technology, designed to makes day-to-day work easier and more efficient, can fail or be misused. As a result, a project run by the BSI and involving the BBK, the Senate Department of Health and Social Care in Berlin and the BG Hospital Berlin (UKB) examined the IT security of hospitals. Results from this project were published in 2013 as a "Hospital IT Risk Analysis" guide, also available as a summary (cf. BSI 2013b).

The step-by-step methods described in this guide can be used to identify and evaluate critical IT dependencies in a hospital and the resulting risks posed.

These findings help facilitate informed decisions regarding which measures should be taken to mitigate the risk of security and safety failures in hospitals. To set out the requirements facing IT security in hospitals that are subject to the *BSI Critical Infrastructure Ordinance,* the "Medical Provisions" branch group of UP KRITIS has developed a health sector-specific security standard, which has since been presented in certified form (DKG 2019; → Chapter 2.2.1 and Infobox 16).

Ensuring hospital care lies within the remit of Germany's constituent states. The *Federal Civil Protection and Disaster Assistance Act* states that the authorities responsible in accordance with state law have to plan additional measures to ensure healthcare provision to the population in a situation of tension or defence. This also governs incident notification and response planning in hospitals (KAEP), which should be structured as uniformly as possible across Germany, taking civil protection aspects into account (→ Chapter 2.3.2). With this in mind, the BBK published a handbook on KAEP in 2020. To compile the handbook, know-how from across Germany was brought together in a working group consisting of leading experts on KAEP.

These included professionals from the German Society of Hospital Disaster Response Planning (DAKEP) and the German Trauma Society (DGU), as well as from the regional states involved. The handbook resulting from this collaboration addresses methodological aspects of the two aforementioned publications and supplements them to provide a comprehensive tool. The aim is to allow hospital operators to independently develop a structured and systematic KAEP tailored to their own hospital, so that the capacity and functionality of hospitals can be maintained in disaster situations. This should in turn facilitate smooth-running processes in the event of a major incident occurring, both within the hospitals themselves and in cooperation with the authorities and defence organisations involved. The handbook will be brought out by the BBK as part of a series and will be provided free of charge.

Figure 27: Imaging technology is just one of many IT-supported procedures in hospitals (source: Tom Werner / DigitalVision / Getty Images).

2.5.5 A resilient transport system: the BMVI Network of Experts "Knowledge – Ability – Action"

The Federal Ministry of Transport and Digital Infrastructure (BMVI) set up the BMVI Network of Experts to bring together the skills and expertise of seven departmental research facilities and executive agencies (cf. Figure 28). The objective is to use research relating to different modes of transport to help ensure that the transport system is both environmentally compatible and resilient to extreme incidents. The BMVI Network of Experts addresses the handling of extreme incidents in an interdisciplinary and intermodal way, taking the various stages of risk and crisis management (preparation, protection, reaction, etc.) into account.

The work of the BMVI Network of Experts is based around several topics. Of these, Topic 1 – "Adapting Transport and Infrastructure to Climate Change and Extreme Weather Events" – and Topic 3 – "Increasing the Reliability of Transport Infrastructures" – are closely linked to the objectives of critical infrastructure protection. Projects from Topic 1 include, for example, analysing the impact of extreme events caused by climate change (e.g. flooding and droughts, storms, landslides, heatwaves, etc.) on different modes of transport and projecting how these will change over the short and long term. Based on this information, scientists from the BMVI Network of Experts are developing examples of mitigation options for road, waterways, and rail (→ Infobox 8). Topic 3 focuses on developing methods to estimate the quantitative impact of extreme events on different elements of the transport infrastructure, such as tunnels, bridges or locks. Further information can be found on the Network of Experts' website (www.bmvi-expertennetzwerk.de).

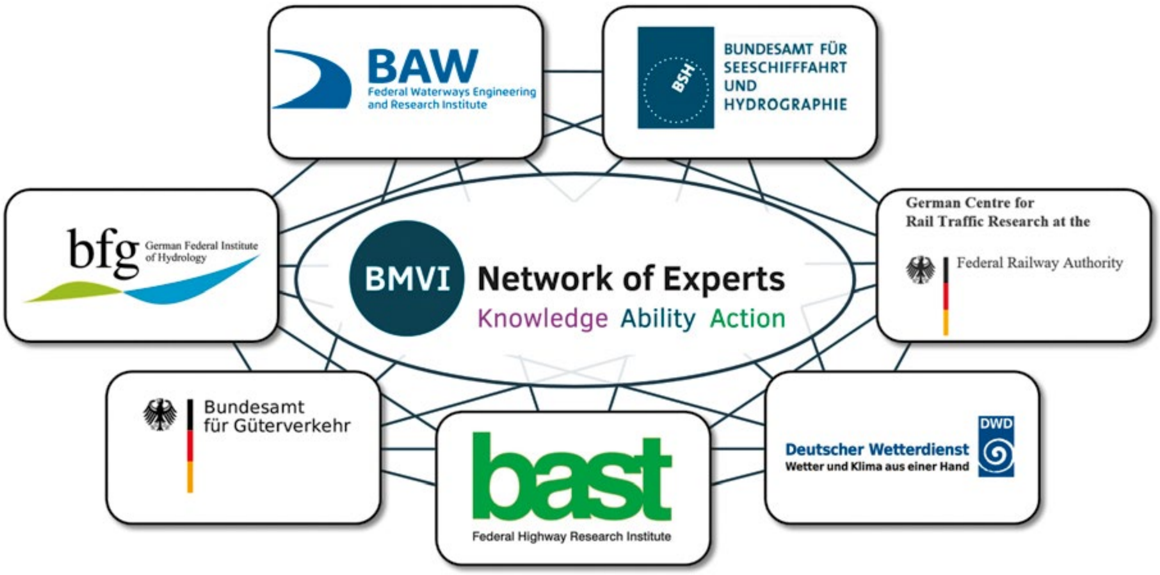

BAW
Federal Waterways Engineering and Research Institute
BSH
BUNDESAMT FÜR SEESCHIFFFAHRT UND HYDROGRAPHIE
bfg German Federal Institute of Hydrology
BMVI Network of Experts
Knowledge Ability Action
German Centre for Rail Traffic Research at the Federal Railway Authority
Bundesamt für Güterverkehr
bast
Federal Highway Research Institute
Deutscher Wetterdienst
Wetter und Klima aus einer Hand
DWD

Figure 28: Overview of the departmental research institutes and executive agencies involved in the BMVI Network of Experts (source: BMVI, translated by: BMVI).

2.6

Chapter

Source: Fabian Wentzel / E+ / Getty Images

Cross-border cooperation in the field of critical infrastructure protection

Neither threats nor infrastructure facilities observe national borders and, in our global economy, services transcend national economic areas. Common security systems are required in order to maintain cross-border services and flows of goods. In this regard, critical infrastructure protection is gaining increasing importance from a cross-border point of view.

The need for cross-border cooperation within Europe is reflected in three of the four fundamental freedoms of the European internal market, to which signatories have been bound by treaty: the freedom to provide services, the free movement of goods, and the free movement of capital and payments as these form the constitutional basis of the European Union. A shared basic understanding of infrastructure security between all member states is vital when it comes to safeguarding the functioning of trans-European transport, energy, and telecommunications networks as part of the European internal market. In response to the terrorist attacks that took place on September 11th 2001 on the one hand, and the challenges posed by digitalisation on the other, the European Commission has developed cross-sector initiatives to protect European and national critical infrastructures and also influenced national legislation (→ Chapter 2.6.1).

Bilateral collaboration is also of great importance – it is often performed as part of reciprocal contracts, agreements or policy statements and put into practice by means of work programmes. The scope and intensity of the cooperation varies and, depending on the agreement, ranges from a sharing of information and experience, to specific projects, to training and education programmes lasting several years. The “D-A-CH format” cooperation, which dates back to 2008, sees participants from Germany, Austria, and Switzerland discuss programme-related considerations, methodological approaches, and tangible measures, as well as the differences and similarities in critical infrastructure protection (→ Chapter 2.6.2).

Finally, cooperation within international organisations is also a key component of strengthening critical infrastructure protection at a national level (→ Chapter 2.6.3). Germany is a member of international bodies including the North Atlantic Treaty Organization (NATO) and the Organisation for Economic Cooperation and Development (OECD), and also participates in the further development of critical infrastructure protection within these frameworks.

2.6.1 Critical infrastructure protection within the European Union

Two milestones have shaped both cooperation on critical infrastructure protection at the European level and national legislation over the long term (→ Chapter 2.2.1): the “European Programme for Critical Infrastructure Protection” (EPCIP) and the *Directive concerning measures for a high common level of security of network and information systems across the Union,* otherwise known as the “NIS Directive” (2016/11487/EU).

The publication of the European Commission’s communication on “Critical Infrastructure Protection in the fight against terrorism” (KOM 2004) in 2004 marked the start of an intense consultation process. This continued with a “Green Paper on a European Programme for Critical Infrastructure Protection” (KOM 2005), published in 2005, and resulted in a “Communication from the Commission on a European Programme for Critical Infrastructure Protection” (KOM 2006). As part of this programme, the *Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* – the so-called “EPCIP Directive” (2008/114/EC) was passed in 2008.

The directive aims to identify and designate European critical infrastructures (ECI), whose degradation would have a significant impact on at least two member states.

It does not concern all of the CI sectors addressed by the Commission, but it is limited to the *energy* and *transport and traffic* sectors. The directive had to be ratified in national law by the start of 2011 and member states did this in various ways: while some chose to pass their own implementation laws, Germany opted for an exclusively technical and legislative path by amending the *Energy Industry Act* (→ Infobox 5). The directive asserts that member states must use both criteria applying across sectors and to specific sectors to identify potential ECI and to then conduct an information and consultation process with those member states affected by potential failures occurring in these sectors. ECI operators need to draw up security plans and appoint a security officer. Member states must provide regular reports to the Commission concerning the status of the implementation and findings from sector-specific risk and threat analyses.

The directive is the only binding EPCIP measure. However, communication and the sharing of best practices at the European level were ultimately spurred on by its non-binding elements, such as regular meetings of national contact points that also act as points of contact for the Commission and other member states, the establishment of the "Critical Infrastructure Warning Information Network" information platform (CIWIN), and the "Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" research programme (CIPS).

Within Germany, the EPCIP Directive led to some irritation but also served to spark discussions. The directive's reference to *European* critical infrastructures did not match with the understanding of the term at the national level. Furthermore, the restriction of the directive to just two sectors led to a need to explain how this applied to sectors considered at the national level (→ Infobox 2). The identification of national critical infrastructures was also considered to have been to some extent "completed" with reference to the implementation of the directive. Nevertheless, the directive's implementation has led to the adoption of legal regulations governing critical infrastructure protection, and to the strategic and legal handling of the issue in other member states.

The NIS Directive (2016/11487/EU), which was passed in 2016, chose a different way to address critical infrastructure protection at the European level: supported by the European Union's regulatory competence on the internal market, this addressed *national* critical infrastructures and included measures to protect these against IT and cyber threats. As a result, it created a uniform legal framework for the EU-wide development of national capacities in cyber security, improved cooperation between the member states, as well as minimum security requirements, and established reporting obligations for operators of critical infrastructures and particular providers of digital services, such as cloud services and online marketplaces.

The directive had to be ratified by member states by May 2018. Germany was prepared for this thanks to its *IT Security Law,* which was passed on 25th July 2015 (→ Chapter 2.2.1). It already contained many of the measures stipulated in the directive and was supplemented with the *BSI Critical Infrastructure Ordinance* to create an instrument for the legally binding identification of critical infrastructures (→ Infobox 16). Regulatory elements of the NIS directive that were not covered, particularly those concerning digital services, were implemented through the *Law on the implementation of the European Directive concerning measures for a high common level of security of network and information systems across the Union.*

The so-called "NIS platform" (ENISA n.d.) was launched in 2013. This did not come about as a result of the NIS Directive, but was intended to be a building block in the IT security policy area. This forum allows public and private sector actors to share experiences about network and information security at the European level, including those regarding incentives for establishing appropriate risk management, for introducing security norms (minimum standards) or for EU-wide voluntary certification schemes. At the EU level, the policy area is framed by the "Cybersecurity Strategy of the European Union" (KOM 2013), published by the Commission in 2013.

2.6.2 Looking to the neighbours: trilateral cooperation with Austria and Switzerland (D-A-CH)

Joint workshops on critical infrastructure protection have been taking place between the German, Austrian, and Swiss authorities every two or three years since 2008. Talking with our neighbours, who are not only connected to us in terms of a shared language but also with regard to their federal structures, has proven ever more rewarding over time.

The aim of this cooperation was, and remains, to sound out the similarities and differences in the field of critical infrastructure protection, particularly those pertaining to the federal systems; to present methods and projects; and to learn from one another, both through examples of best practice and by discussing common challenges faced. The idea is for representatives of the coordinating bodies to meet up. For Germany this includes staff from the BMI, BBK, and BSI. For Austria, the Federal Ministry for the Interior, the Federal Chancellery, and the Federal Office for the Protection of the Constitution and Counterterrorism take part; in Switzerland the Federal Office of Civil Protection participates. Other relevant specialist offices and ministries are also welcome and have joined the discussions on specific themes.

Four two-day sessions have taken place to date. The first workshop was used for position fixing and included presentations on the current state of play. The agenda for the subsequent sessions has included national programmes, procedures for identifying critical infrastructures and the topics of risk analysis, crisis communication, and resilience indicators. The meetings have taken the format of workshops from their inception.

The latest projects concerning a specific focus are presented and the methodological approaches of the individual countries are compared and discussed in view of how they can be implemented elsewhere. The issue of whether critical infrastructure protection in Germany and Austria has developed differently from the Swiss experience due to the mandatory implementation of EU law in the former has led to extremely interesting discussions – it was concluded that this has not yet been the case. The results of the last two meetings were documented in detail with the help of the Center for Security Studies of the Swiss Federal Institute of Technology in Zurich (Herzog/Roth 2014; Maduz/Roth 2018).

2.6.3 Critical infrastructure protection in international organisations

Cooperation within international organisations also plays a key role in enhancing critical infrastructure protection at the national level. Germany is a member of international organisations, including the North Atlantic Treaty Organization (NATO) and the Organisation for Economic Cooperation and Development (OECD). Germany is also involved in the further development of critical infrastructure protection within this framework – although the term used within NATO and OECD circles is “resilience” of critical infrastructures.

Critical infrastructure protection has been on NATO’s agenda for many years. This can be seen with the setting up of an “Ad hoc Working Group on Critical Infrastructure Protection” as early as 2001. NATO and non-NATO states have also been collaborating and sharing experiences and best practice on critical infrastructure protection within the framework of the “Partnership for Peace”, which has been in operation since the 1990s (NATO 2017).

The topic was also given a more binding character, largely through resolutions made at the 2014 NATO summit in Wales (NATO 2014) that relate to the impact of the conflict in the Ukraine on civil emergency planning and civil protection.

NATO’s Resilience Directives, passed in 2016, define seven “Baseline Requirements” for providing critical services (NATO 2016). These must be provided by NATO member states in order to guarantee their duties – for example, in conjunction with the “Host Nation Support” – the support of allied or friendly armed forces in their own country. The Baseline Requirements also define guidelines and criteria that member states can use to evaluate their preparation measures.

NATO formulates the Baseline Requirements as follows:

- assured continuity of government and critical government services
- resilient energy supplies
- ability to deal effectively with the uncontrolled movement of people
- resilient food and water resources
- ability to deal with mass casualties
- resilient civil communications systems
- resilient civil transportation systems

(NATO 2016; NATO 2018)

The Baseline Requirements drawn up by NATO relate to seven of the nine CI sectors addressed in Germany (→ Infobox 2). As such, they also provide impetus for critical infrastructure protection at the national level and for crisis management within the framework of civil defence (→ Chapter 2.3.2). Experts from NATO member states met in working groups organised by specific topics (for instance, the "Joint Health Agriculture and Food Group") to set out the requirements facing member states formulated in the Baseline Requirements.

The OECD regularly brings together representatives from member states' responsible executive bodies in its "High Level Risk Forum". This collaboration has led to the "Policy Toolkit", published in 2019, which is a summary of recommendations and policy instruments under the title "Good Governance for Critical Infrastructure Resilience" (OECD 2019). The Policy Toolkit explains how the resilience of critical infrastructures can be enhanced in a dynamic risk landscape and presents seven steps that can help to increase the resilience of critical infrastructures at the national level. These include establishing a cross-sector approach, establishing trust between authorities and operators, and taking into account cross-border challenges. Many of these steps had already been implemented or initiated in Germany for critical infrastructure protection. However, this does not mean that there is little to learn from others. The OECD provides a platform for sharing knowledge between its members, with a focus on examples of best practice from different countries. The intention is for as many countries as possible to benefit from the experiences of other members of the organisation and to be able to adapt tried-and-tested concepts from other countries to their own national conditions.

3

Chapter

Source: Yuji Kotani / DigitalVision / Getty Images

Outlook

The insights into the implementation of the CIP Strategy summarised in Chapter 2 show that critical infrastructure protection has moved forward a great deal since 2009. How will things progress from here? What will shape the field of critical infrastructure protection over the next five to ten years? It is already possible to identify some of the topics that will play a key role in the near future. One thing is clear: just as the world is in a state of flux, so, too, is critical infrastructure protection an evolving phenomenon.

Global trends offer opportunities – and risks

There are enormous expectations associated with the growing use of information technology through the course of digitalisation and with innovative technologies, such as artificial intelligence. Keeping an eye on the new dependencies between infrastructure systems and vulnerabilities in the supply of critical services that are to be expected with these changes will become an increasingly important part of critical infrastructure protection. The desirable parts of these technical advancements need to be exploited, while at the same time potential risks need to be identified and minimised.

Climate change is also one of the global developments that will demand the attention of everyone involved in critical infrastructure protection, both now and in the future. It is likely not only to necessitate adaptive measures in this country, but also a widespread “world of infrastructure” at the global level. Changes to the international security situation also have consequences for critical infrastructure protection: cyber and hybrid threats have become increasingly significant in recent years and there is nothing to suggest that this situation will change soon.

When it comes to the developments cited here (that may be yet to unfold), the following applies: the ability to identify changes at an early stage, to make prognoses, and to issue “early warnings” concerning the dynamic risks facing the supply of critical services must be continuously developed and expanded upon.

The focus is increasingly on system resilience

In terms of the resilience of critical infrastructures, the focus is on the ability to withstand various risks and/or to be able to respond to them flexibly. This applies both to individual facilities and to entire infrastructure systems and their associated processes. Taking into account the technological developments described above and the current rate of digitalisation, we must assume that interdependencies between critical infrastructures will continue to increase. The provision of critical services always depends on a number of interlinked process and infrastructure components. In light of these developments, critical infrastructure protection will involve paying closer attention to the resilience of infrastructure systems in order to ensure the reliable provision of critical services.

Taking a more systematic viewpoint raises questions as to which services and infrastructures count as critical. For example, satellite-based services in several branches of critical infrastructures have continued to grow in importance. As a result, the classification of sectors and branches from 2011 is now in need of revision and should be updated in line with current requirements. Discussions surrounding this requirement will increasingly include findings from both regional and local levels as well as on the federal stage.

The horizontal and vertical networking of state actors is being developed further

Cooperation between actors at all levels of administration and with executive responsibility for the various sectors is essential to critical infrastructure protection. There remains great potential to use cooperation between authorities to plan and make decisions that span different legal fields and, in this way, to develop a shared understanding of critical infrastructure protection as a cross-sectoral task.

Critical infrastructure facilities are “physically” located within local authorities and are generally subject to local supervision. At the same time, infrastructure systems cross administrative borders and the provision of critical services is pervaded by a network of technical regulations that transcend levels. Thus, in addition to horizontal cooperation, vertical cooperation between federal, state, and local authorities is vital. Authorities across all levels can only create the framework for a resilient provision of critical services by working together.

Key insights regarding the development of the strategic foundations for critical infrastructure protection are currently provided by the working group for the critical infrastructure protection liaison office at the federal and state levels. This working group is due to continue its work with a stronger connection to the interior department's committee structure and has set itself the aim of drawing up a joint federal and regional critical infrastructure protection strategy. From this, it is apparent that the federal government's CIP Strategy could soon be replaced by a national strategic policy. As such, the development of this and discussions regarding it between administrative levels and departments will form a vital focus of the work over the coming years.

Integrated risk and crisis management: Cooperation between state and private actors remains the central task

Cooperation between state and private actors – already a key aspect of critical infrastructure protection – will continue to grow in importance in the future. A systematic sharing of information and best practices is the only way to ensure that everyone involved is best able to contribute to increasing the resilience of critical infrastructures. The form of cooperative lawmaking that was chosen in the course of drawing up the *IT Security Law* has proven its worth in the cooperation between the state and private industry, and this should be continued wherever feasible.

Many of the activities described in Chapter 2 can be subsumed under the term ”integrated risk and crisis management“. In line with the cooperative approach, this includes measures implemented by the state and measures taken by the operators of critical infrastructures. Experiences from recent years have shown how vital it is that operators and state actors work together in all phases of the risk and crisis management process, from prevention to reaction. Developing this integrated approach further and applying it across all levels are tasks for the next decade.

Cooperating also means communicating (or being in a position to do so). As such, improving communication, especially that between security services, civil protection workers, and operators of critical infrastructures, will be a key task for the coming years. The safeguarding of technical means of communication will play a role along with the discussion of processes and the clarification of differences in the language culture of different actors.

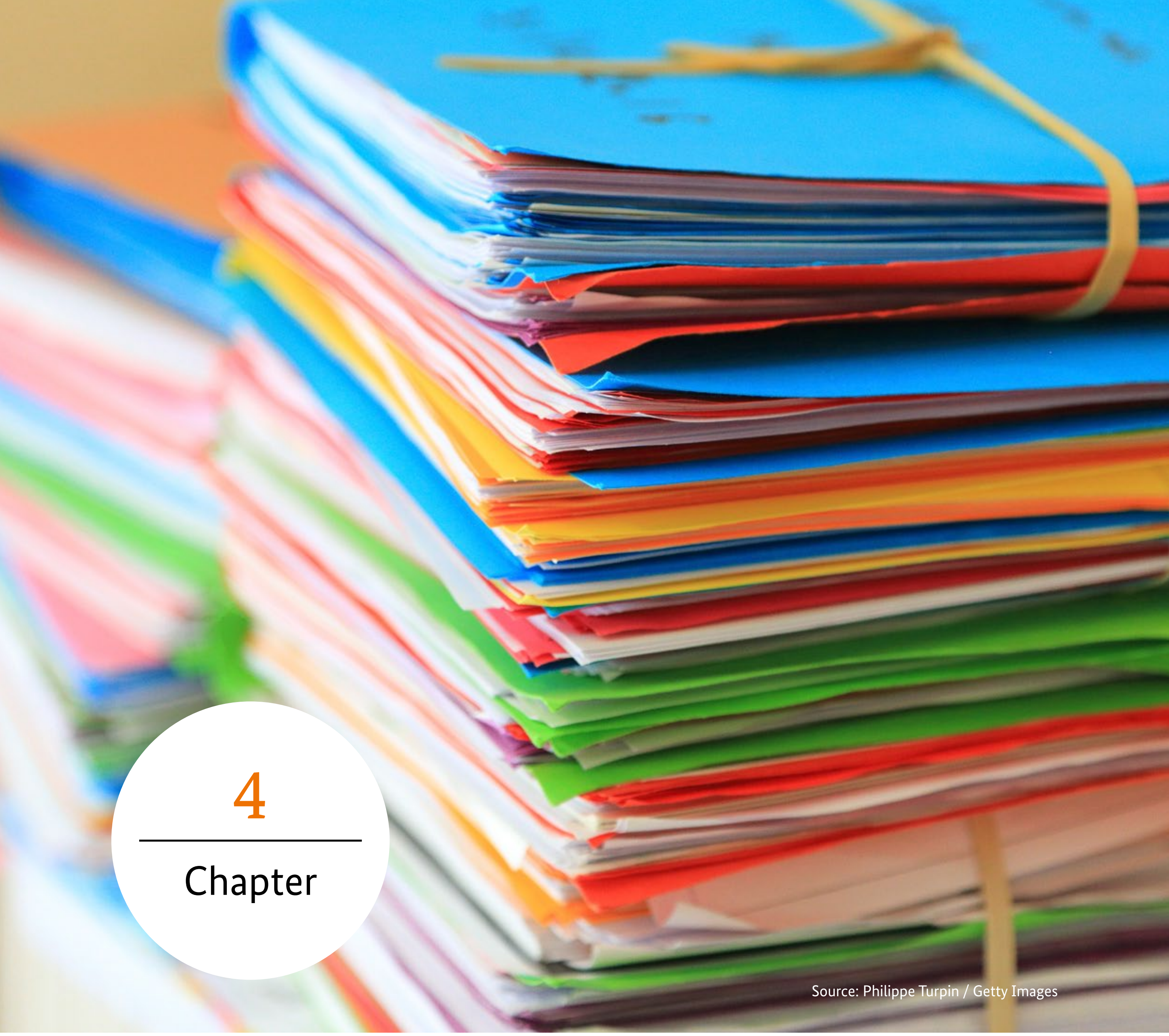
Collaborative formats, such as discussion platforms and round tables, are key instruments when it comes to structuring this cooperation and ensuring a trusting exchange between the various actors.

UP KRITIS has become established as a central platform for cooperation between the federal institutions and operators of critical infrastructures; however, more and more collaborative formats are being set up across all levels. Both existing and new formats need to be strengthened and developed further. The Sendai Framework for Disaster Risk Reduction can act as an initiator here over the coming years – at the national level and beyond.

Critical infrastructure protection must be structured at the international level

The EU will continue to have a considerable influence on critical infrastructure protection within the member states and therefore in EU associate states as a whole. This can already be seen in the recommendations for further legislative acts on critical infrastructure protection as well as network and information security. These initiatives must be actively supported and shaped from a German perspective. Germany will also be involved in cooperation between the member states and with the EU, whether through the further development of the "European Programme for Critical Infrastructure Protection" or in the linking of disaster management and critical infrastructure protection. This connection is also likely to be set out in the "Knowledge Network", which is envisaged as part of the EU's Civil Protection Mechanism.

Critical infrastructure protection is increasingly coming to the fore at the United Nations, OECD and NATO levels, too. These organisations formulate requirements for their members with various levels of commitment. The implementation of the United Nations' "Sendai Framework for Risk Reduction", which is already under way in many countries, will provide a variety of starting points for this over the coming years: reducing failures in critical infrastructures is explicitly cited in the framework as a goal. In Germany, NATO's requirements are addressed by the Civil Defence Concept and its implementation will, therefore, also be reflected in activities concerning critical infrastructure protection in Germany for the foreseeable future.



4

Chapter

Source: Philippe Turpin / Getty Images

Indexes

List of abbreviations

AG KOST KRITIS
Arbeitsgruppe der Koordinierungsstellen für den Schutz Kritischer Infrastrukturen in Bund und Ländern
(The critical infrastructure protection liaison office's working group at the federal and regional levels)

AG KRITIS
Arbeitsgruppe Kritische Infrastrukturen
(Critical infrastructures working group)

AKNZ
Akademie für Krisenmanagement, Notfallplanung und Zivilschutz
(Academy for Crisis Management, Emergency Planning and Civil Protection)
Information: In 2021 the name was changed to Federal Academy of Civil Protection and Civil Defence (BABZ).

Art.
Article

ASG
Arbeitssicherstellungsgesetz
(Labour Protection Act)

AWV
Außenwirtschaftsverordnung
(German Foreign Trade and Payments Ordinance)

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht
(Federal Financial Supervisory Authority)

BAIT
Bankaufsichtliche Anforderungen an die IT
(Supervisory Requirements for IT in Financial Institutions)

BAK
Branchenarbeitskreis
(Industry working group) (in UP KRITIS)

BBK
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
(Federal Office of Civil Protection and Disaster Assistance)

BBR
Bundesamt für Bauwesen und Raumordnung
(Federal Office for Building and Regional Planning)

BBSR
Bundesinstitut für Bau-, Stadt- und Raumforschung
(Federal Institute for Research on Building, Urban Affairs and Spatial Development)

B3S
branchenspezifischer Sicherheitsstandard
(Industry-specific security standards)

BfDI
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
(Federal Commissioner for Data Protection and Freedom of Information)

BKM
Beauftragte der Bundesregierung für Kultur und Medien
(Representative of the Federal Ministry for Culture and the Media)

BLE
Bundesanstalt für Landwirtschaft und Ernährung
(Federal Office for Agriculture and Food)

BLG
Bundesleistungsgesetz
(Federal Requisitioning Law)

BMBF
Bundesministerium für Bildung und Forschung
(Federal Ministry of Education and Research)

BMI
Bundesministerium des Innern
(Federal Ministry of the Interior)
Since 2018: Bundesministerium des Innern für Bau und Heimat
(Federal Ministry of the Interior, Building and Community)

BMU
Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit
(Federal Ministry for the Environment, Nature Conservation and Nuclear Safety)

BMVI
Bundesministerium für Verkehr und digitale Infrastruktur
(Federal Ministry of Transport and Digital Infrastructure)

BMWi
Bundesministerium für Wirtschaft und Energie
(Federal Ministry for Economic Affairs and Energy)

BNetzA
Bundesnetzagentur
(Federal Network Agency)

BSI
Bundesamt für Sicherheit in der Informationstechnik
(Federal Office for Information Security)

BSIG
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
(Act on the Federal Office for Information Security)

BSI-KritisV
BSI-Kritisverordnung
(BSI Critical Infrastructure Ordinance)

BT-Drs.
Bundestagsdrucksache
(parliamentary documents)

CI
Critical infrastructure(s)

CI operators
Operators of critical infrastructures

CIP
Critical infrastructure protection

CIPS
Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks

CI sectors
Sectors of critical infrastructure systems

CIP Strategy
Nationale Strategie zum Schutz Kritischer Infrastrukturen
(National Strategy for Critical Infrastructure Protection)

CSS
Cyber-Sicherheitsstrategie für Deutschland
(Cyber Security Strategy for Germany)

CIWIN
Critical Infrastructure Warning Information Network

D-A-CH
Germany-Austria-Switzerland

DAKEP
Deutsche Arbeitsgemeinschaft Krankenhaus-Einsatzplanung e. V.
(German Society of Hospital Disaster Response Planning)

DAS
Deutsche Anpassungsstrategie an den Klimawandel
(German Strategy for Adaptation to Climate Change)

DGU
Deutsche Gesellschaft für Unfallchirurgie
(German Trauma Society)

DigiNetzG
Gesetz zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze
(Law to facilitate the expansion of digital high-speed networks)

DIN
Deutsches Institut für Normung e. V.
(German Institute for Standardisation)

DIN SPEC
DIN specification

DKG
Deutsche Krankenausgesellschaft e. V.
(The German Hospital Federation)

DVGW
Deutscher Verein des Gas- und Wasserfaches e. V.
(German Association for Gas and Water)

DWA
Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V.
(German Association for Water, Wastewater and Waste)

ECI
European critical infrastructure(s)

ENISA
European Union Agency for Cybersecurity

EnSiG
Energiesicherungsgesetz
(Energy Security Act)

ENTSO-E
European Network of Transmission System Operators for Electricity

ENTSO-G
European Network of Transmission System Operators for Gas

EnWG
Energiewirtschaftsgesetz
(Energy Industry Act)

EPCIP
European Programme for Critical Infrastructure Protection

ErdölBevG
Erdölbevorratungsgesetz
(Petroleum Stockholding Act)

ESVG
Ernährungssicherstellungs- und -vorsorgegesetz
(Emergency Food Control Act and Emergency Food Supply Act)

EU
European Union

FNN
Forum Netztechnik/Netzbetrieb im VDE
(Forum Network Technology/Network Operation)

GG
Grundgesetz
(Basic Law for the Federal Republic of Germany)

ggf.
gegebenenfalls

GGO
Gemeinsame Geschäftsordnung der Bundesministerien
(Joint Rules of Procedure of the Federal Ministries)

IMK
Ständige Konferenz der Innenminister und -senatoren der Länder (Innenministerkonferenz)
(Standing Conference of State Interior Ministers and Senators)

IMK 's working group AK V
Ständige Konferenz der Innenminister und -senatoren der Länder (Innenministerkonferenz), Arbeitskreis V – Feuerwehrangelegenheiten, Rettungswesen, Katastrophenschutz und zivile Verteidigung
(Standing Conference of State Interior Ministers and Senators, working group V – Fire Fighting Issues, Rescue Services, Disaster Prevention and Civil Defense)

ISO
International Organization for Standardization

IT
Information technology

IT-SiG
IT-Sicherheitsgesetz
(IT Security Law)

KAIT
Kapitalverwaltungsaufsichtliche Anforderungen an die IT
(Supervisory Requirements for IT in German Asset Managers)

KAEP
Krankenhausalarm- und -einsatzplanung
(Incident notification and response planning in hospitals)

KNK
Konferenz Nationaler Kultureinrichtungen
(Conference of National Cultural Institutions)

KomPass
Kompetenzzentrum Klimafolgen und Anpassung im UBA
(Competence centre for "Climate Impacts and Adaptation in Germany")

kVA
kilovolt-ampere

KZV
Konzeption Zivile Verteidigung
(Civil Defence Concept)

LÜKEX
Länder- und Ressortübergreifende Krisenmanagementübung (Exercise)
(Interstate and Interministerial Crisis Management Exercise)

MaRisk
Mindestanforderungen an das Risikomanagement (im Kredit- und Finanzdienstleistungswesen)
(Minimum Requirements for Risk Management in banking and financial services)

MORO
Modellvorhaben der Raumordnung
(Demonstration Projects of Spatial Planning)

NATO
North Atlantic Treaty Organization

NKS
Nationale Kontaktstelle für das Sendai Rahmenwerk für Katastrophenvorsorge
(Office of the National Focal Point for the Sendai Framework)

NPSI
Nationaler Plan zum Schutz der Informationsinfrastrukturen
(National Plan for Information Infrastructure Protection)

OECD
Organisation for Economic Cooperation and Development

PG KRITIS
Projektgruppe Kritische Infrastrukturen
(Critical infrastructures project group)

PTSG
Post- und Telekommunikationssicherstellungsgesetz
(Post and Telecommunications Security Act)

SiFo
Sicherheitsforschungsprogramm
(Security Research Programme)

SiLK
SicherheitsLeitfaden Kulturgut
(Guidelines for the Protection of Cultural Property)

TAB
Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag
(Office of Technology Assessment at the German Bundestag)

TAK
Themenarbeitskreis
(Topic working group) (in UP KRITIS)

THW
Bundesanstalt Technisches Hilfswerk
(Federal Agency for Technical Relief)

THWG
THW-Gesetz
(THW Law)

TKG
Telekommunikationsgesetz
(Telecommunications Act)

UBA
Umweltbundesamt
(German Environment Agency)

UKB
Unfallkrankenhaus Berlin
(BG Hospital Berlin, hospital for accident cases)

UN DRR (former UN ISDR)
United Nations Office for Disaster Risk Reduction
(former United Nations International Strategy for Disaster Reduction)

UNESCO
United Nations Educational, Scientific and Cultural Organization

UP KRITIS
Prior to 2014: Umsetzungsplan KRITIS (CIP Implementation Plan, for NPSI); since then, proper name

VAIT
Versicherungsaufsichtliche Anforderungen an die IT
(Supervisory Requirements for IT in Insurance Undertakings)

VDE
Verband der Elektrotechnik Elektronik Informationstechnik e. V.
(Association for Electrical, Electronic & Information Technologies)

VerkLG
Verkehrsleistungsgesetz
(Transportation Provision Act)

VerkSiG
Verkehrssicherstellungsgesetz
(Transport Security Act)

WasSiG
Wassersicherstellungsgesetz
(Water Security Act)

WiSiG
Wirtschaftssicherstellungsgesetz
(Economic Security Act)

Y2K
Year 2000 (“millennium issue”)

ZSKG
Zivilschutz- und Katastrophenhilfegesetz
(Federal Civil Protection and Disaster Assistance Act)

List of references

Index of cited publications and online sources

ARL 2011 – Akademie für Raumforschung und Landesplanung (2011): Zukünftige Ausgestaltung des Risikomanagements in der Raumplanung. Positionspapier aus der ARL. Nr. 86. Hannover.

BaFin 2017 – Bundesanstalt für Finanzdienstleistungsaufsicht (2017): Mindestanforderungen an das Risikomanagement (MaRisk). Rundschreiben 09/2017 (BA) vom 27.10.2017.

> English version available: Federal Financial Supervisory Authority (2017): Annex 1: Annotated text of the Minimum Requirements for Risk Management (MaRisk) in the version of 27.10.2017.
> Online available on: https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs0917_marisk_Endfassung_2017_pdf_ba_en.pdf?__blob=publicationFile&v=5 (27.10.2021).

BaFin 2018a – Bundesanstalt für Finanzdienstleistungsaufsicht (2018a): Bankaufsichtliche Anforderungen an die IT (BAIT). Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018.

> English version available: Federal Financial Supervisory Authority (2018): Supervisory Requirements for IT in Financial Institutions. Bankaufsichtliche Anforderungen an die IT – BAIT in the version of 14.09.2018.
> Online avaiable on: https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1710_ba_BAIT_en.pdf?__blob=publicationFile&v=6 (27.10.2021).

BaFin 2018b – Bundesanstalt für Finanzdienstleistungsaufsicht (2018): Kritische Infrastrukturen: BaFin ergänzt BAIT um KRITIS-Modul. Internetmeldung vom 14.09.2018.
Online available on: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung_180914_Ueberarbeitung_BAIT.html (27.10.2021).

BaFin 2019a – Bundesanstalt für Finanzdienstleistungsaufsicht (2019a): Versicherungsaufsichtliche Anforderungen an die IT (VAIT). Rundschreiben 10/2018 (VA) in der Fassung vom 20.03.2019.

> English version available: Federal Financial Supervisory Authority (2019): Supervisory Requirements for IT in Insurance Undertakings. Versicherungsaufsichtliche Anforderungen an die IT – VAIT in the version of 20.03.2019.
> Online available on: https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1810_vait_va_en.pdf?__blob=publicationFile&v=6 (27.10.2021).

BaFin 2019b – Bundesanstalt für Finanzdienstleistungsaufsicht (2019b): Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT). Rundschreiben 11/2019 (WA) in der Fassung vom 01.10.2019.

> English version available: Federal Financial Supervisory Authority (2019): Supervisory Requirements for IT in German Asset Managers (Kapitalverwaltungsaufsichtliche Anforderungen an die IT – KAIT). Circular 11/2019 (WA) in the version of 01.10.2019.
> Online available on: https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1911_KAIT_en.pdf?__blob=publicationFile&v=3 (27.10.2021).

BBK 2005 – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2005): Problemstudie Risiken für Deutschland (Teil 1 und 2). Bad Neuenahr-Ahrweiler.

BBK 2008 – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens. Bonn.

BBK 2010 – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2010): Neue Strategie zum Schutz der Bevölkerung in Deutschland. Bonn.

BBK 2012 – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2012): Schutzkonzepte Kritischer Infrastrukturen im Bevölkerungsschutz. Ziele, Zielgruppen, Bestandteile und Umsetzung im BBK. Bonn.

BBK 2015a – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2015a): Notstromversorgung in Unternehmen und Behörden. Leitfaden für die Planung, die Einrichtung und den Betrieb einer Notstromversorgung in Unternehmen und Behörden. Bonn.

BBK 2015b – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2015b): Was tun bei Stromausfall – Vorsorge und Selbsthilfe. (Published: 01.10.2015).
Online available on: https://youtu.be/VijPkjKVv9I (27.10.2021).

BBK 2015c – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2015c): Was tun bei Stromausfall – Strom selbst erzeugen. (Published: 29.10.2015).
Online available on: https://youtu.be/3XCTa1mkAWc (27.10.2021).

BBK 2017 – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2017): Treibstoffversorgung bei Stromausfall. Empfehlung für Zivil- und Katastrophenschutzbehörden. Bonn.

BBK 2018a – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2018a): Bevölkerungsschutz. Ausgabe 3/2018. (Themenheft: Integriertes Risikomanagement).

BBK 2018b – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2018b): Autarke Notstromversorgung der Bevölkerung. Bonn.

BBK 2019a – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019a): Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten. Bonn.

> English version available: Federal Office of Civil Protection and Disaster Assistance (2019): Protecting Critical Infrastructures – A Seven Step Identification Process Guidance tool for use in civil protection. Bonn.

BBK 2019b – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019b): Auswertungsbericht LÜKEX 18. Gasmangellage in Süddeutschland. Gas Supply Shortage in Southern Germany. Comprehensive Report on Findings – English Summary included. Bonn.

BBK 2019c – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019c): Stromausfall. Vorsorge und Selbsthilfe. Bonn.

BBK 2019d – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019d): Sicherheit der Trinkwasserversorgung. Teil 1: Risikoanalyse. Bonn.

BBK 2019e – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019e): Sicherheit der Trinkwasserversorgung. Teil 2: Notfallvorsorgeplanung. Bonn.

BBK 2019f – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019f): BBK-Glossar. Ausgewählte zentrale Begriffe des Bevölkerungsschutzes. Bonn.

BBK/BSI 2011 – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik (2011): Sektoren und Branchen Kritischer Infrastrukturen (Internetmeldung, Stand: 13.5.2011).

BMBF 2007 – Bundesministerium für Bildung und Forschung (2007): Forschung für die zivile Sicherheit. Programm der Bundesregierung. Bonn.

BMBF 2015 – Bundesministerium für Bildung und Forschung (2015): Selbstbestimmt und sicher in der digitalen Welt 2015-2020. Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit. Bonn.

BMBF 2018 – Bundesministerium für Bildung und Forschung (2018): Forschung für die zivile Sicherheit 2018–2023. Rahmenprogramm der Bundesregierung. Bonn.

BMI 2005a – Bundesministerium des Innern (2005a): Schutz Kritischer Infrastrukturen – Basisschutzkonzept. Empfehlungen für Unternehmen. Berlin.

> English version available: Federal Ministry of the Interior (2005): Protection of Critical Infrastructures – Baseline Protection Concept. Recommendation for Companies. Berlin.
> Online available on: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/Basisschutzkonzept_kritische_Infrastrukturen_en.pdf?__blob=publicationFile&v=1 (27.10.2021).

BMI 2005b – Bundesministerium des Innern (2005b): Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI). Berlin.

> English version available: Federal Ministry of the Interior (2005): National Plan for Information Infrastructure Protection. Berlin.
> Online available on: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KRITIS/National_Plan_for_Information_Infrastructure_Protection.pdf?__blob=publicationFile&v=1 (27.10.2021).

BMI 2007a – Bundesministerium des Innern (2007a): Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen. Berlin.

> English version available: Federal Ministry of the Interior (2007): CIP Implementation Plan of the National Plan for Information Infrastructure Protection. Berlin.

BMI 2007b – Bundesministerium des Innern (2007b): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden. Berlin.

BMI 2009 – Bundesministerium des Innern (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Berlin.

English version available: Federal Ministry of the Interior (2009): National Strategy for Critical Infrastructure Protection (CIP Strategy). Berlin.
Online available on: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v= (27.10.2021).

BMI 2011a – Bundesministerium des Innern (2011a): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden. Berlin.

BMI 2011b – Bundesministerium des Innern (2011b): Cyber-Sicherheitsstrategie für Deutschland. Berlin.

English version available: Federal Ministry of the Interior (2011): Cyber Security Strategy for Germany. Berlin.

BMI 2016a – Bundesministerium des Innern (2016a): Cyber-Sicherheitsstrategie für Deutschland 2016. Berlin.

English version available: Federal Ministry of the Interior (2016): Cyber Security Strategy for Germany 2016. Berlin.
Online available on: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/5f3c65fe954c4d33ad6a9242cd5bb448/file_en (27.10.2021).

BMI 2016b – Bundesministerium des Innern (2016b): Konzeption Zivile Verteidigung. Berlin.

BMI 2017 – Bundesministerium des Innern (2017): Umsetzungsplan Bund 2017. Leitlinie für Informationssicherheit in der Bundesverwaltung. Berlin.

BMVg 2016 – Bundesministerium der Verteidigung (2016): Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr. Berlin.

English version available: Federal Ministry of Defence (2016): White Paper 2016 on German Security Policy and the Future of the Bundeswehr. Berlin.
Online available on: https://www.bundeswehr.de/resource/blob/4800140/fe103a80d8576b2cd7a135a5a8a86dde/download-white-paper-2016-data.pdf (27.10.2021).

BMVg 2018 – Bundesministerium der Verteidigung (2018): Konzeption der Bundeswehr. Berlin.

BMVI 2014 – Bundesministerium für Verkehr und digitale Infrastruktur (2014): Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft. Schutz kritischer Infrastrukturen und verkehrsträgerübergreifende Gefahrenabwehr. Berlin.

BMVI 2017 – Bundesministerium für Verkehr und digitale Infrastruktur (2017): Handbuch zur Ausgestaltung der Hochwasservorsorge in der Raumordnung. MORO Regionalentwicklung und Hochwasserschutz in Flussgebieten. Berlin.

BMVI/BBSR 2015 – Bundesministerium für Verkehr und digitale Infrastruktur; Bundesinstitut für Bau-, Stadt- und Raumforschung (2015): Endbericht zu Modellvorhaben der Raumordnung (MORO) Vorsorgendes Risikomanagement in der Regionalplanung (AZ 10.05.06-13.6).

BNetzA 2015 – Bundesnetzagentur (2015): IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz. (Stand: August 2015).

BNetzA 2016 – Bundesnetzagentur (2016): Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG). (Stand: Juli 2016).

BNetzA 2018 – Bundesnetzagentur (2018): IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz. (Stand: Dezember 2018).

BReg 2008 – Bundesregierung (2008): Deutsche Anpassungsstrategie an den Klimawandel vom Bundeskabinett am 17. Dezember 2008 beschlossen. Berlin.

> English version available: The Federal Government (2008): German Strategy for Adaptation to Climate Change adopted by the German federal cabinet on 17th December 2008. Berlin.
> Online available on: https://www.bmu.de/fileadmin/bmu-import/files/english/pdf/application/pdf/das_gesamt_en_bf.pdf (27.10.2021).

BReg 2015 – Bundesregierung (2015): Fortschrittsbericht zur Deutschen Anpassungsstrategie an den Klimawandel. Stand: 16.11.2015. Berlin.

> English summary available: Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety (BMUB) (2016): Adaptation to Climate Change. Initial Progress Report by the Federal Government on Germany's Adaptation Strategy. Berlin.
> Online available on: https://www.bmu.de/fileadmin/Daten_BMU/Pools/Broschueren/fortschrittsbericht_anpassung_klimawandel_en_bf.pdf (27.10.2021).

BSI 2004 – Bundesamt für Sicherheit in der Informationstechnik (2004): Jahresbericht 2003. Bonn.

> English version available: Federal Office for Information Security (BSI) (2004): Annual Report 2003. Berlin.
> Online available on: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Annualreport/BSI-AnnualReport2003_pdf.pdf;jsessionid=24EDC8842190E60B9CD3AC4363A46B17.internet462?__blob=publicationFile&v=1 (27.10.2021).

BSI 2013a – Bundesamt für Sicherheit in der Informationstechnik (2013a): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Leitfaden. Bonn.

BSI 2013b – Bundesamt für Sicherheit in der Informationstechnik (2013b): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Management-Kurzfassung. Bonn.

BSI 2017a – Bundesamt für Sicherheit in der Informationstechnik (2017a): Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS. Bonn.

BSI 2017b – Bundesamt für Sicherheit in der Informationstechnik (2017b): Merkblatt zum sicheren Informationsaustausch mit TLP 17-11. Bonn.

ENISA n.d. – European Union Agency for Cybersecurity (n.d.): NIS-Platform.
Online available on: https://resilience.enisa.europa.eu/nis-platform (27.10.2021)

Fekete et al. 2019 – Fekete, A.; Neisser, F.; Tzavella, K.; Hetkämper, C. (2019; Eds.): Wege zu einem Mindestversorgungskonzept. Kritische Infrastrukturen und Resilienz, Köln.

Herzog/Roth 2014 – Herzog, M.; Roth, F. (2014): Dritter D-A-CH Workshop Schutz Kritischer Infrastrukturen, 4.-6. Dezember 2013, Magglingen. Zürich.

IMK 2009 – Ständige Konferenz der Innenminister und -senatoren der Länder (2009): Programm Innere Sicherheit. Fortschreibung 2008/2009. Potsdam.

KNK n.d. – Konferenz Nationaler Kultureinrichtungen (n.d.): SiLK – SicherheitsLeitfaden Kulturgut.
Abrufbar unter: http://www.konferenz-kultur.de/SLF/index1.php (27.10.2021)

> English version available: German Conference of National Cultural Institutions (Konferenz Nationaler Kultureinrichtungen / KNK) (n.d.): SiLk – Guildelines for the protection of cultural property.
> Online available on: http://www.konferenz-kultur.de/SLF/EN/index1.php?lang=en (27.10.2021).

KOM 2004 – Kommission der Europäischen Gemeinschaften (2004): Mitteilung der Kommission zum Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung. KOM(2004)702. 20.10.2004. Brüssel.

> English version available: Commission of the European Communities (2004): Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the fight against terrorism. COM(2004) 702. From 20.10.2004. Brussels.
> Online available on: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2004)702&lang=en (27.10.2021).

KOM 2005 – Kommission der Europäischen Gemeinschaften (2005): Grünbuch über ein Europäisches Programm für den Schutz kritischer Infrastrukturen. KOM(2005)576. 17.11.2005, Brüssel.

> English version available: Commission of the European Communities (2005): Green Paper on a European Programme for Critical Infrastructure Protection. COM(2005) 576. From 17.11.2005. Brussels.
> Online available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN (27.10.2021).

KOM 2006 – Kommission der Europäischen Gemeinschaften (2006): Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen. KOM(2006)786. 12.12.2006. Brüssel.

> English version available: Commission of the European Communities (2006): Communication from the Commission on a European Programme for Critical Infrastructure Protection. Com(2006) 786. From 12.12.2006. Brussels.
> Online available on: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2006)786&lang=en (27.10.2021).

KOM 2013 – Europäische Kommission (2013): Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum. JOIN(2013)1. 07.02.2013. Brüssel.

> English version available: European Commission (2013): Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013)1. From 07.02.2013. Brussels.
> Online available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=DE (27.10.2021).

Lechner et al. 2018 – Lechner, U.; Dännert, S.; Rieb, A.; Rudel, S. (2018; Eds.): CASE|KRITIS. Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. Berlin.

Maduz/Roth 2018 – Maduz, L.; Roth, F. (2018): Vierter Trilateraler Workshop D-A-CH Schutz kritischer Infrastrukturen", 4.-6. Juni 2018 in Bonn. Zürich.

NATO 2014 – North Atlantic Treaty Organization (2014): Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. Press release (2014/120) from 05.09.2014.

NATO 2016 – North Atlantic Treaty Organization (2016): Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016. Press release (2016/118) from 08.07.2016.

NATO 2017 – North Atlantic Treaty Organization (2017): Partnership for Peace Programme. (Version: 07.06.2016).

NATO 2018 – North Atlantic Treaty Organization (2018): Resilience and Article 3. (Version: 03.12.2019).

NKS 2019 – Nationale Kontaktstelle für das Sendai Rahmenwerk beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019): Sendai Rahmenwerk für Katastrophenvorsorge 2015-2030. Bonn.

> English version available: UN 2015 - UNISDR (2015): Sendai Framework for Disaster Risk Reduction 2015 - 2030. Geneva.

OECD 2019 – Organisation for Economic Co-operation and Development (2019): Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies. Paris.

PCCIP 1997 – President's Commission on Critical Infrastructure Protection (1997): Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection. Washington.

Rudel/Lechner 2018 – Rudel, S.; Lechner, U. (2018; Eds.): IT-Sicherheit für Kritische Infrastrukturen – State of the Art. Ergebnisse des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen ITS|KRITIS des BMBF. München.

THW 2014 – Bundesanstalt Technisches Hilfswerk (2014): Katalog der Einsatzoptionen des THW. (Version: November 2014). Bonn.

UP KRITIS 2008a – Geschäftsstelle des UP KRITIS (2008a): Früherkennung und Bewältigung von IT-Krisen, Bonn.

UP KRITIS 2008b – Geschäftsstelle des UP KRITIS (2008b): IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen. Bonn.

UP KRITIS 2014a – Geschäftsstelle des UP KRITIS (2014a): UP KRITIS. Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen. Bonn.

English version available: Geschäftsstelle des UP KRITIS (2014): UP KRITIS. Public-Private Partnership for Critical Infrastructure Protection. Bonn.

UP KRITIS 2014b – Geschäftsstelle des UP KRITIS (2014b, Fortschreibung): Früherkennung und Bewältigung von IT-Krisen. Bonn.

UP KRITIS 2014c – Geschäftsstelle des UP KRITIS (2014c, Fortschreibung): IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen. Bonn.

Index of Legal Sources

Aktiengesetz (German Stock Corporation Act, AktG) from 6th September 1965 (BGBl. I p. 1089), last modified by Art. 1 of the law from 12th December 2019 (BGBl. I p. 2637).

Arbeitssicherstellungsgesetz (Labour Security Act, ASG) from 9th July 1968 (BGBl. I p. 787), last modified by Art. 24 of the law from 4th August 2019 (BGBl. I p. 1147).

Außenwirtschaftsverordnung (German Foreign Trade and Payments Ordinance, AWV) from 2nd August 2013 (BGBl. I p. 2865), last changed by Art. 1 of the ordinance from 27th February 2019 (BAnz AT 06.03.2019 V1).

Bundesleistungsgesetz (Federal Requisitioning Law, BLG) in the Bundesgesetzblatt (German Federal Law Gazette) Part III, Classification Number 54-1, published version, last modified by Art. 5 of the law from 11th August 2009 (BGBl. I p. 2723).

Energiesicherungsgesetz (Energy Security Act, EnSiG) 1975 from 20th December 1974 (BGBl. I p. 3681), last modified by Art. 324 of the ordinance from 31st August 2015 (BGBl. I p. 1474).

Energiewirtschaftsgesetz (Energy Industry Act, EnWG) from 7th July 2005 (BGBl. I p. 1970, 3621), last modified by Art. 1 of the law from 13th May 2019 (BGBl. I p. 706).

Erdölbevorratungsgesetz (Petroleum Stockholding Act, ErdölBevG) from 16th January 2012 (BGBl. I p. 74), last modified by Art. 127 of the law from 29th March 2017 (BGBl. I p. 626).

Ernährungssicherstellungsgesetz (Emergency Food Control Act, ESG) in the version published on 27th August 1990 (BGBl. I p. 1802), last modified by Art. 359 of the ordinance from 31st August 2015 (BGBl. I p. 1474), replaced on 11th April 2017 by the Gesetz zur Neuregelung des Rechts zur Sicherstellung der Ernährung in einer Versorgungskrise (Act to Revise the Law on Food Control in a Supply Crisis) from 4th April 2017.

Ernährungssicherstellungs- und -vorsorgegesetz (Emergency Food Control Act and the Emergency Food Supply Act, ESVG) from 4th April 2017 (BGBl. I p. 772).

Ernährungsvorsorgegesetz (Emergency Food Supply Act, EVG) from 20th August 1990 (BGBl. I p. 1766), last modified by Art. 362 of the ordinance from 31st August 2015 (BGBl. I p. 1474), replaced on 11th April 2017 by the Gesetz zur Neuregelung des Rechts zur Sicherstellung der Ernährung in einer Versorgungskrise (Act to Revise the Law on Food Control in a Supply Crisis) from 4th April 2017.

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (Act on the Federal Office for Information Security, BSI-Gesetz, BSIG) from 14th August 2009 (BGBl. I p. 2821), last modified by Art. 1 of the law from 23rd Juni 2017 (BGBl. I p. 1885).

Gesetz über das Technische Hilfswerk (Federal Agency for Technical Relief Act, THW-Gesetz, THWG) from 22nd January 1990 (BGBl. I p. 118), last modified by Art. 5 of the law from 11th June 2013 (BGBl. I p. 1514).

Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Federal Civil Protection and Disaster Assistance Act, ZSKG) from 25th March 1997 (BGBl. I p. 726), last modified by Art. 2(1) of the law from 29th July 2009 (BGBl. I p. 2350).

Gesetz über die Errichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (Act on the Establishment of the Federal Office of Civil Protection and Disaster Assistance) from 27th April 2004 (BGBl. I p. 630).

Gesetz zu der Konvention vom 14. Mai 1954 zum Schutz von Kulturgut bei bewaffneten Konflikten (Law on the Convention of 14th May 1954 for the Protection of Cultural Property in the Event of Armed Conflict) from 11th April 1967 (BGBl. 1967 II p. 1233), last modified by Art. 3 of the law from 31st July 2016 (BGBl. I p. 1914).

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT Security Law, IT-SiG) from 17th July 2015 (BGBl. I p. 1324).

Gesetz zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze (Law to facilitate the expansion of digital high-speed networks, DigiNetzG) from 4th November 2016.

Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 23. Juni 2017 (Law on the implementation of the Directive of the European Parliament and of the Council from 6th July 2016 concerning measures for a high common level of security of network and information systems across the Union from 23rd June 2017) (BGBl. I p. 1885).

Grundgesetz für die Bundesrepublik Deutschland (Basic Law of the Federal Republic of Germany, GG) in the Bundesgesetzblatt (German Federal Law Gazette) Part III, Classification Number 100-1, published version, last modified by Art. 1 of the law from 28th March 2019 (BGBl. I p. 404).

Gemeinsame Geschäftsordnung der Bundesministerien (Joint Rules of Procedure of the Federal Ministries, GGO) from 1st September 2011.

Post- und Telekommunikationssicherstellungsgesetz (Post and Telecommunications Security Act, PTSG) from 24th March 2011 (BGBl. I p. 506, 941), modified by Art. 7 of the law from 4th November 2016 (BGBl. I p. 2473).

COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (ABl. L 345 from 23.12. 2008, p. 75).

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (ABl. L 194 from 19.07.2016, p. 1).

Raumordnungsgesetz (German Spatial Planning Act, ROG) from 22nd December 2008 (BGBl. I p. 2986), last modified by Art. 2(15) of the law from 20th July 2017 (BGBl. I p. 2808).

Telekommunikationsgesetz (Telecommunications Act, TKG) from 22nd June 2004 (BGBl. I p. 1190), last modified Art. 12 of the law from 11th July 2019 (BGBl. I p. 1066).

Verkehrsleistungsgesetz (Transportation Provision Act, VerkLG) from 23rd July 2004 (BGBl. I p. 1865), last modified by Art. 15 of the law from 26th July 2016 (BGBl. I p. 1843).

Verkehrssicherstellungsgesetz (Transport Security Act, VerkSiG) in the version published on 8th October 1968 (BGBl. I p. 1082), last modified by Art. 499 of the ordinance from 31st August 2015 (BGBl. I p. 1474).

Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending regulation (EU) No. 646/2012 (ABl. L 176 from 27.06.2013, p. 1).

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI Critical Infrastructure Ordinance, BSI-KritisV) from 22nd April 2016 (BGBl. I p. 958), modified by Art. 1 of the ordinance from 21st June 2017 (BGBl. I p. 1903).

Wassersicherstellungsgesetz (Water Security Act, WasSiG) from 24th August 1965 (BGBl. I p. 1225, 1817), last modified by Art. 2(20) of the law from 12th August 2005 (BGBl. I p. 2354).

Wirtschaftssicherstellungsgesetz (Economic Security Act, WiSiG) in the version published on 3rd October 1968 (BGBl. I p. 1069), last modified by Art. 262 of the ordinance from 31st August 2015 (BGBl. I p. 1474).

Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Hazardous Incident Ordinance, 12. BImSchV) in the version published on 15th March 2017 (BGBl. I p. 483), last modified by Art. 1a of the ordinance from 8th December 2017 (BGBl. I p. 3882).

Index of Cited Parliamentary Documents

BT-Drs 15/2286: Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes über die Errichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (22.12.2003).

BT-Drs. 17/5672: Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung. Technikfolgenabschätzung (TA). TA-Projekt: Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung (27.04.2011).

BT-Drs. 17/12051: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2012 (03. 01. 2013).

BT-Drs. 18/208: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2013 (16.12.2013).

BT-Drs. 18/3682: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2014 (23.12.2014).

BT-Drs. 18/7209: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2015 (04.01.2016).

BT-Drs. 18/8332: Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze (DigiNetzG) (04.05.2016).

BT-Drs. 18/10850: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2016 (28.12.2016).

BT-Drs. 19/5920: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2017 (12.04.2019).

BT-Drs. 19/9521: Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2018 (12.04.2019).

Index of Cited Norms, Standards and Regulations

BSI-Standard 200-2 “IT-Grundschutz-Methodik“ (IT Baseline Security) (Version 1.0).
English version available: BSI-Standard 200-2 “IT-Grundschutz Methodology” (Version 1.0).
Online available on: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.pdf;jsessionid=6A565169F8278012BCB0AB9F32BD9708.internet482?__blob=publicationFile&v=2 (28.10.2021).

DIN EN 15975-1:2016-03 “Sicherheit der Trinkwasserversorgung – Leitlinien für das Risiko- und Krisenmanagement – Teil 1: Krisenmanagement” (Security of the Drinking Water Supply – Guidelines for Risk and Crisis Management – Part 1: Crisis Management) (from: 03/2016).

DIN EN 15975-2:2013-12 “Sicherheit der Trinkwasserversorgung – Leitlinien für das Risiko- und Krisenmanagement – Teil 2: Risikomanagement” (Security of the Drinking Water Supply – Guidelines for Risk and Crisis Management – Part 2: Risk Management) (from: 12/2013).

DIN ISO 31000:2018-10 “Risikomanagement – Leitlinien” (Risk management – Guidelines) (from: 10/2018).

DIN SPEC 91390:2019-12 “Integriertes Risikomanagement für den Schutz der Bevölkerung” (Integrated Risk Management in Civil Protection) (from: 12/2019).

DKG 2019 – Deutsche Krankenausgesellschaft (The German Hospital Federation) (2019): Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (Industry-specific security standard for healthcare provision in hospitals). Berlin. (from: 22.10.2019).

DVGW G 1003 (M) Technischer Hinweis – Merkblatt “Hinweise für die Aufrechterhaltung der sicheren Gasversorgung bei Ausfall der regulären Kommunikation” (Code of Practice for Maintaining a Secure Gas Supply in the Event of a Failure of Regular Communication) (from: 07/2019).

DVGW W 1060:2017-08 Merkblatt “IT-Sicherheit – Branchenstandard Wasser/ Abwasser” (Code of Practice on: IT security – industry standard for water/wastewater) (from: 08/2017).

DWA M 551 Merkblatt Audit “Hochwasser – wie gut sind wir vorbereitet” (Audit “Flooding – how well-prepared are we?”) (from: 12/2010).

DWA M 1060:2017-08 Merkblatt “IT-Sicherheit – Branchenstandard Wasser/ Abwasser” (Code of Practice on: IT security – industry standard for water/wastewater) (from: 08/2017).

Index of Cited Research Projects

AISIS: Automatisierte Informationsgewinnung und Schutz kritischer Infrastruktur im Katastrophenfall. Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/schutz-von-verkehrsinfrastrukturen/aisis/aisis-automatisierte-informati-rastruktur-im-katastrophenfall.html (29.10.2021).

AISTEC: Bewertung alternder Infrastrukturbauwerke mit digitalen Technologien. Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/verkehrsinfrastrukturen/aistec/aistec-bewertung-alternder-inf-rke-mit-digitalen-technologien.html (29.10.2021).

AlphaKomm: Ausfallsichere Lagebildinformationen zur Kommunikation im Krisenfall. Project description: https://www.sifo.de/sifo/de/projekte/schutz-und-rettung-von-menschen/schutz-und-rettung-bei-komplexen-einsatzlagen/alphakomm/alphakomm-ausfallsichere-lageb-ur-kommunikation-im-krisenfall.html (29.10.2021).

AquaBioTox: Onlinefähige Trinkwasserüberwachung mittels eines biologischen Breitbandsensors. Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/detektion-von-gefahrstoffen/aquabiotox/aquabiotox-onlinefaehige-trink-t-automatischer-bildauswertung.html (29.10.2021).

AQUA-IT-Lab: Labor für IT-Sicherheit bei Wasserversorgern. Project description: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/aqua-it-lab (29.10.2021).

AURIS: Autonomes Risiko-und Informationssystem zur Strukturanalyse und Überwachung sicherheitsrelevanter Bauwerke. Project description: https://www.sifo.de/sifo/shareddocs/datei/projektumriss_auris_svv-pdf.pdf?__blob=publicationFile&v=2 (29.10.2021).

ESecLog: Erweiterte Sicherheit in der Luftfrachtkette. Project description: https://www.sifo.de/sifo/shareddocs/datei/projektumriss_eseclog-pdf.pdf?__blob=publicationFile&v=2 (29.10.2021).

INDI: Intelligente Intrusion-Detection-Systeme für Industrienetze. Project description: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/indi (29.10.2021).

InfoStrom: Lernende Informationsinfrastrukturen für das Krisenmanagement am Beispiel der Stromversorgung. Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/schutz-vor-ausfall-von-versorgungsinfrastrukturen/infostrom/infostrom-lernende-information-m-beispiel-der-stromversorgung.html (29.10.2021).

Kat-Leuchttürme: KatastrophenschutzLeuchttürme als Anlaufstelle für die Bevölkerung in Krisensituationen.
Project description: https://www.sifo.de/sifo/de/projekte/gesellschaft/sicherheitsoekonomie-und-sicherheitsarchitektur/kat-leuchttuerme/kat-leuchttuerme-katastrophens-oelkerung-in-krisensituationen.html (29.10.2021).

KIRMin: Kritische Infrastruktur – Resilienz als Mindestversorgungskonzept.
Project description: https://www.sifo.de/sifo/de/projekte/schutz-und-rettung-von-menschen/erhoehung-der-resilienz/kirmin/kirmin-kritische-infrastruktur--als-mindestversorgungskonzept.html (29.10.2021).

MIME: Multimodales Mustererkennungssystem zum Schutz der Bevölkerung vor organisierter Arzneimittelkriminalität.
Project description: https://www.sifo.de/sifo/shareddocs/datei/projektumriss_mime-pdf.pdf?__blob=publicationFile&v=2 (29.10.2021).

NeuENV: Neue Strategien der Ernährungsnotfallvorsorge.
Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/sicherung-der-lebensmittel-und-lebensmittelwarenketten/neuenv/neuenv-neue-strategien-der-ernaehrungsnotfallvorsorge.html (21.10.2021).

PREPARED^{NET}: Agentenbasierte Simulation und Erforschung eines Notfallkonzeptes zum Schutz von sensiblen Logistikknoten.
Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/sicherung-der-warenketten/preparednet/preparednet-agentenbasierte-si-z-von-sensiblen-logistikknoten.html (29.10.2021).

PREVIEW: Resilienz kritischer Verkehrsinfrastrukturen am Beispiel der Wasserstraßen.
Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/verkehrs-infrastrukturen/preview-resilienz-kritischer-v-am-beispiel-der-wasserstrassen/preview-resilienz-kritischer-v-am-beispiel-der-wasserstrassen.html (29.10.2021).

QPASS: Quick Personnel Automatic Safe Screening.
Project description: https://www.sifo.de/sifo/shareddocs/datei/projektumriss_qpass-pdf.pdf?__blob=publicationFile&v=2 (29.10.2021).

RESCUE IT: IT¬-Plattform für die lückenlose Sicherung von Lebensmittelwarenketten.
Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/sicherung-der-warenketten/rescue-it/rescue-it-it-plattform-fuer-di-ng-von-lebensmittelwarenketten.html (02.11.2021).

ResiWater: Innovative, sichere Sensornetzwerke und modell-gestützte Bewertungs- und Analyse-Tools zur Erhöhung der Resilienz von Trinkwasserinfrastrukturen.
Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen/resiwater/resiwater-innovative-sichere-s-von-trinkwasserinfrastrukturen.html (02.11.2021).

SafeMed: Systemgestaltung zur wirtschaftlichen Sicherung der Medikamentenversorgung.
Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/sicherung-der-warenketten/safemed/safemed-systemgestaltung-zur-w-ung-der-medikamentenversorgung.html (02.11.2021).

SiLeBAT: Sicherstellung der Futter und Lebensmittelwarenkette bei bio und agroterroristischen (BAT)-Schadenslagen.
Project description: https://www.sifo.de/sifo/shareddocs/datei/projektumriss_silebat-pdf.pdf?__blob=publicationFile&v=2 (02.11.2021).

STATuS: Schutz der Trinkwasserversorgung in Hinblick auf CBRN-Bedrohungsszenarien – Phase 2. Project description: https://www.sifo.de/sifo/shareddocs/datei/projektumriss_status-pdf.pdf?__blob=publicationFile&v=2 (02.11.2021).

TankNotStrom: Energie- und Kraftstoffversorgung von Tankstellen und Notstromaggregaten bei Stromausfall
Project description: https://www.sicherheit-forschung.de/forschungsforum/zukunftslabor-sicherheit/Projekte_im_zlab/Projektumriss_TankNotStrom.pdf (29.10.2021)

VeSiKi: Vernetzte IT-Sicherheit Kritischer Infrastrukturen (Begleitforschungsprojekt des Förderschwerpunktes IT-Sicherheit für Kritische Infrastrukturen).
Project description: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/vesiki (29.10.2021).

VESPER: Verbesserung der Sicherheit von Personen in der Fährschifffahrt.
Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/schutz-von-verkehrsinfrastrukturen/vesper/vesper-verbesserung-der-sicher-rsonen-in-der-faehrschifffahrt.html (02.11.2021).

VESPERPLUS: Verbesserung der Sicherheit von Personen in der Fährschifffahrt.
Project description: https://www.sifo.de/sifo/shareddocs/datei/projektumriss_vesperplus-pdf.pdf?__blob=publicationFile&v=2 (02.11.2021).

ZEBBRA: Zustandserfassung und -bewertung von Brücken basierend auf Radar-Sensorik in Kombination mit intelligenten Algorithmen.
Project description: https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/verkehrsinfrastrukturen/zebbra-zustandserfassung-und-b--mit-intelligenten-algorithmen/zebbra-zustandserfassung-und-b--mit-intelligenten-algorithmen.html (02.11.2021).

Index of Illustrations

Imprint

Publisher

Federal Office of Civil Protection
and Disaster Assistance
Postfach 1867, 53008 Greven

Tel. +49 (0)228 99 550-0

www.bbk.bund.de

Editorial team:

Susanne Krings, Federal Office of Civil Protection and Disaster Assistance, Dept. II.3

Typesetting

ORCA Affairs GmbH, Schumannstraße 5, 10117 Berlin

Printing

WM-Druck + Verlag, Römerkanal 52, 53359 Rheinbach

Compiled

Februar 2020

Circulation

1000

Image credits

Title photo: Anthony Rakusen / Cultura / Getty Images
Page 6: Mutzberg, BBK

ISBN 978-3-939347-95-8

This volume represents the opinion of the authors and does not reflect the opinion of the editor.

www.bbk.bund.de