13 Secure Critical Infrastructures

Jonas Franken and Christian Reuter

Abstract

Critical infrastructures (CI) provide societies with essential goods and services. With the growing impact of digitalisation, information and communication technologies play an increasing role within these entities. Large-scale outages in many of the ten German CI sectors revealed the increasing vulnerabilities stemming from dependencies on electricity and connectivity. While the CI concept is widely used in current public debates, some inconsistencies require nuanced attention from students and researchers of CI. This chapter introduces secure critical infrastructures. It therefore provides an overview of the central characteristics, essential concepts of hierarchy, (inter-)dependency, criticality, and vulnerability to enable a coherent analysis of CI. To map out the multi-actor landscape within CI, the private, public, hybrid and civil-society stakeholders mainly shaping CI policies and discourses will be introduced.

J. Franken (✉) · C. Reuter
Science and Technology for Peace and Security (PEASEC),
Technische Universität Darmstadt, Darmstadt, Germany
e-mail: franken@peasec.tu-darmstadt.de

C. Reuter
e-mail: reuter@peasec.tu-darmstadt.de

C. Reuter (ed.), *Information Technology for Peace and Security*,
Technology, Peace and Security I Technologie, Frieden und Sicherheit,
https://doi.org/10.1007/978-3-658-44810-3_13

Objectives

- Understanding the critical infrastructure concept and what generally characterises infrastructure.
- Gaining knowledge of the common critical infrastructure sectors and the role of IT within each.
- Comprehension of four core concepts of critical infrastructure research: hierarchies, (inter-)dependency, vulnerability, and criticality.
- Overviewing the complex, multi-level actor arrangements of critical infrastructure protection.

13.1 Introduction to Critical Infrastructures

In order to approach the concept of critical infrastructures, in this chapter, we first take an in-depth look at the concept's origin and the different definitions that have been established for it. The term Critical Infrastructure (CI) is a composite expression that draws its etymological roots from two key concepts: **criticality** and **infrastructure**. The prefix *infra* is derived from Latin, meaning "below" or "beneath", highlighting the underlying and fundamental role that these entities play in the functioning of society. "Structure", on the other hand, is associated with the arrangement and construction of something intentional and human-made. The word critical traces its origins to the Greek *kritikós*, denoting the ability to discern, emphasising the decisive roles of these infrastructures compared to others. Therefore, CI conveys the notion of essential arrangements vital to a society's functioning, reflecting their crucial importance in various domains of life. The usage of CI emerged from military post-WWII security concepts as a framework for civil defence and has experienced a rise in recent decades (Collier & Lakhoff, 2008).

Today's definitions for CI vary in detail but have important core concepts (see Table 13.1). They usually mention an asset, structure, facility, system, equipment, function, or parts thereof that may be physical, organisational, or virtual. CI are not technical arrangements alone but also entail social and cultural aspects. For these entities to qualify as critical, definitions refer either to their status as **providers** of essential services or the severity of the consequences of their failure.[1] Additionally, some definitions mention specific referent objects, e.g. public health, public safety, national (economic) security, commerce, the environment, society, or a combination thereof. Critics of the concepts view its gaps in the state-centricity, represented by the former three referent objects. These standard definitions may neglect infrastructural systems and practices crossing territorial borders or referent objects beyond a state's direct reach, for example, low-earth orbit satellite constellations or submarine data cables.

[1] For a comprehensive overview of current CI definitions, see CIPedia (Fraunhofer IAIS, 2019).

Table 13.1 Definition of CI of international, regional, and national actors

Organization	Definition
United Nations Office for Disaster Risk Reduction (UNDRR)	Critical facilities: The primary **physical structures, technical facilities and systems** which are **socially, economically or operationally** essential to the functioning of a **society or community**, both in routine circumstances and in the extreme circumstances of an emergency. (UNISDR, 2009)
International Telecommunication Union (ITU)	Critical Infrastructure: The **key systems, services and functions** whose disruption or destruction would have a debilitating impact on **public health and safety, commerce, and national security, or any combination of these.** (ITU, 2008)
European Commission	'Critical infrastructure' means an **asset, a facility, equipment, a network or a system, or a part of** an asset, a facility, equipment, a network or a system, which is necessary for the **provision of an essential service**. (EU-Directive 2022/2557, 2022)
North Atlantic Treaty Organisation	Critical Infrastructure: **Physical or virtual systems and assets** under the jurisdiction of a State that are so vital that their incapacitation or destruction may debilitate a **state's security, economy, public health or safety, or the environment**. (M. N. Schmitt, 2017)
German Federal Government	Critical infrastructures (CI) are **organisational and physical structures and facilities** of such vital importance to a nation's **society and economy** that their failure or degradation would result in sustained supply shortages, significant disruptions of **public safety and security**, or other dramatic consequences. (Federal Ministry of the Interior, 2009)
United States Government	**Systems and assets, whether physical or virtual**, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on **security, national economic security, national public health or safety, or any combination of those matters.** (NIST, 2020)

13.2 Characteristics of Infrastructures

Star and Ruhleder (1996, p. 114) consider a different perspective on infrastructures. They ask the question "*when is infrastructure*" instead of "*what is an infrastructure*". Following this perspective, Susan Leight Star's (1999) study of infrastructure ethnography identifies essential characteristics of infrastructure that not only shed light on its nature and functioning but also raise the question of when objects take the role of being an infrastructure. These characteristics are instrumental in developing a deeper understanding of the role and challenges of infrastructure:

- An infrastructure is **embedded** in existing social arrangements, structures, and technological contexts. For example, a railway track's architecture is shaped, inter alia, by the social and economic needs along its route, the technical possibilities during planning, and geographic constraints. Thus, it does not exist in isolation but interacts with other elements in a complex way.
- Infrastructure connects to other infrastructure and tools in a **standardised** way. Therefore, it has a significant impact on practice conventions and influences how we perform certain activities.
- Because new infrastructures are **built on an installed** base, older ones often form the foundation for future services and technologies. They inherit strengths and limitations from their base. For example, fibre-optic networks often follow old railway and road infrastructures.
- Infrastructure is fixed in **modular** gradations and cannot be changed all at once or globally. There are technical and structural dependencies that require changes in small steps. For example, the transition to green energy necessitates a substantial number of individual operative actions within the energy sector and beyond before reaching the ultimate objective of carbon-free energy.
- An infrastructure is characterised by **transparency** in the sense of its simplicity in usage. For example, for users to get access to the electricity grid, not more than inserting a plug is required, which leads to **taking** infrastructures and their functioning **for granted**. Users often do not notice it until they lack its services or other problems arise. A typical example is mobile reception, which usually accompanies phone users unnoticed until it is suddenly unavailable – be it in tunnels or rural areas.
- Besides this **temporal reach**, infrastructure has a **spatial distribution** beyond single events or local practices. It can influence how users behave in a particular space or at a particular time. For example, while the European electric grid is a highly regulated and coordinated cross-border network, there is still a considerable variation in the plug types depending on the location. Networked infrastructures can even be international or within areas of no national jurisdiction. For example, submarine data cables in the High Seas – further than 200 nautical miles from coastlines – are governed by the United Nations Convention on the Laws of the Seas, which is an international treaty (Davenport, 2018; McLaughlin et al., 2022). This fact reveals that infrastruc-

tures can well be global, connecting states and societies by circulating goods across borders, oceans, and even airspace and outer space (Bueger et al., 2022; Franken, 2022).

13.3 Critical Infrastructure Sectors

In addition to the definitions, most actors entrusted with CI protection adopt their own classifications of CI into separate sectors. Each country has different schemes for categorising critical infrastructures. The classification in Germany, for example, provides for ten different sectors, which are shown (Fig. 13.1). In addition, important actors, IT systems, and an example of a failure are given for each sector.

The following five sectors can be seen as **technical basic infrastructures** (Federal Ministry of the Interior, 2009, p. 5):

1. The **energy** sector includes the supply of electricity, gas, mineral oil, and district heating. In addition to the large producers of energy, suppliers such as network operators and logistics companies are important players in the sector. It should also be noted that this sector is highly internationalised. For example, the German electricity grid is integrated into the Synchronous grid of Continental Europe, of which all its neighbouring countries are also members. Furthermore, many fossil fuels (mineral oil and gas) come from non-EU countries. The electricity sub-sector hugely depends on functioning IT, as this sector's grid is particularly complex. In the future, increasingly

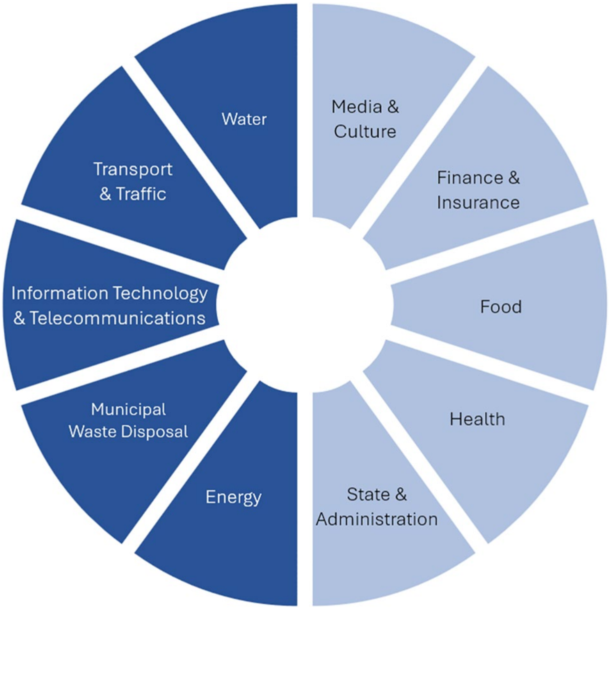

Fig. 13.1 Overview of CI sectors in Germany, distinguished by technical basis infrastructures (dark) and socio-economic service infrastructures (light), modified after BSI (2023)

decentralised energy production will require communication between input and output devices in order to keep grid frequencies constant. Well-known incidents in the energy sector are the power cuts in north-western Germany in 2005 (Klinger et al., 2011), India in 2012 (Blankenship & Urpelainen, 2020), as well as the shortage of mineral oil during the oil price crises of 1973 and 1979 (Mitchell, 2015).

2. The **information technology and telecommunications** sector includes data storage and processing, as well as data transmission, which also covers voice and video. With the rise of IT technology integrated into many areas of life, the criticality of this sector continues to grow. While postal services remain important to society, internet service providers are the ones enabling critical, real-time communications. In addition, the sector can ensure the emergency alert infrastructure that enables communication between the state and citizens during crises. Key players are internet service providers (ISPs), data service providers (data centres, internet exchange points (IXPs), and carriers), and regulatory authorities. Failures in the sector can have a variety of causes. For example, a fire at the Siegen Telekom exchange in 2013 triggered a widespread outage of fixed and mobile networks and the city's websites. A volcanic eruption in 2022 severed the only submarine cable to the Pacific island state of Tonga, resulting in a weeklong national internet outage (Franken et al., 2022; Speidel, 2022). Cyber sabotages, such as the hack of satellite communications provider Viasat, which disrupted around 5800 wind turbines in Germany, can also have a substantial impact (Cyber Peace Institute, 2022a).
3. The **transport and traffic** sector is tasked with ensuring the transportation of material goods and people. This entails providing rail and road transport, inland waterways, maritime shipping, and aviation. Logistics as the organisational background service of the transport sector is also crucial. With the growth of just-in-time delivery, the sector's dependence on IT systems for coordinating and monitoring the flow of goods is particularly increasing. A striking example of the consequences of an accident can be seen in the week-long blockade of the Suez Canal by the container freighter Ever Given in March 2021 (Ramos et al., 2021). The ensuing costs amounted to hundreds of millions USD, and a surge in oil prices was triggered (Reuters, 2021). In 2017, one of the world's largest freight companies, Maersk, suffered a large-scale shutdown due to the NotPetya wiper attack, resulting in additional costs of more than USD 200 million (Jones & Khan, 2021).
4. In Germany, the **water** sector includes fresh water supply and wastewater disposal. Drinking water is vital as a source of food, as well as a means of production and a hygienic requirement for a well-functioning everyday life. In Germany, water collection, treatment, and distribution tend to be provided on a decentralised basis, primarily by municipal utilities. In contrast, other regions of the world have to rely on centrally organised desalination plants due to a shortage of fresh water and require large sewer systems. Pumping systems and net-pressure plants require a power supply to function, and new plants are now digitally controlled (Hassanzadeh et al., 2020). Climate change particularly affects the water sector as it triggers more intense

meteorological events, such as prolonged droughts exhausting reserves, or flash floods, which overburden drainage systems (Kourtis & Tsihrintzis, 2021).

5. The **municipal waste** sector has just been codified as a CI sector in 2021. It includes the collection, recycling, and disposal of solid waste. The stakeholders in this sector range from small to large waste companies, some of which are owned by municipalities themselves. With various waste-to-energy facilities available in Europe, the sector also serves as a source for heat and electricity production. Prolonged failures in this sector create harmful environmental and sanitary conditions, as demonstrated by the frequent waste crises in Naples (Nola et al., 2018). However, dangers also loom in cyberspace. In 2022, for example, a data centre in Darmstadt was hacked, interrupting bulk waste collection in Frankfurt.

The following five sectors form the **socio-economic service infrastructures** (Federal Ministry of the Interior, 2009, p. 5):

6. Banks, financial service providers, stock exchanges, and insurance companies are the key actors in the **finance and insurance** sector. Their task is to ensure daily payment transactions (cash and digital), a stable currency, and insurance services. Cash withdrawal and online banking are now heavily IT-dependent. This effect is reinforced by a decline in traditional bank counters and the increase in online-only banks without any branch structures of their own. As a result of a fundamentally decentralised structure, large-scale cash dispenser failures are rare, given the functioning of electricity and the internet. However, the example of the submarine cable rupture in Tonga in 2022 demonstrates that losing one of these upstream infrastructures can lead to outages of financial transactions lasting several days (Speidel, 2022).
7. At least since the COVID-19 pandemic and its accompanying shortages of medical equipment and vaccines, there has been widespread awareness of the critical infrastructures of the **health** sector. Key players include hospitals, doctors' offices, pharmacies, pharmaceutical companies and wholesalers, and laboratories. The diversity of players and their interconnections lead to high complexity and multiple interdependencies. Health data, such as patient records, is also highly personal, which is why digitalisation solutions in this sector must be designed with high privacy requirements (Cyber Peace Institute, 2022b).
8. The **food** sector is responsible for supplying the population with all types of food. Farmers, food processors, logistics companies, and retailers are central players in maintaining the food supply. Despite its initially relatively hesitant digitisation, all parts of the agricultural supply chains now have IT-supported operations (Kuntke, Linsner, et al., 2022; Kuntke, Romanenko, et al., 2022). The digital solutions range from automated, sensor-heavy smart farming and GPS-assisted precision farming to data-driven product tracking for end customers (Linsner et al., 2021). During the Russian war of aggression against Ukraine, supply shortages occurred in the grain sector due to the blockade of Ukrainian seaports and targeted destruction of storage

facilities. Fewer exports from Ukraine were a factor in regional famines worldwide in 2022 and 2023, especially in the Global South (Mottaleb et al., 2022).

9. In Germany, the **state and administration** sector is divided into four parts: the executive, the legislative, and the judiciary, as well as the emergency and rescue services. Due to the federal structure, the actors in Germany are diverse: federal and state ministries and their subdivided authorities, courts of all levels, and the correctional system, as well as parliaments and municipal bodies. In addition, there are fire departments, rescue services, and disaster control. The availability of these public institutions is an important pillar of internal security because it is a fundamental prerequisite for citizens' trust in the state's ability to act. Thus, IT plays a central role in all these areas, especially in crisis communications. One example of an attack on this CI sector is the 2015 Bundestag hack, in which significant amounts of data from internal parliamentary communications flowed onto foreign servers (Bendiek & Schulze, 2021).
10. The **media and culture** sector ensures the correct communication and preservation of current and historically significant information. In global comparison, this sector from German classification is only rarely mentioned separately. However, it is often included in the former sector, interpreting the provision of neutral media and access to culture as public service (Weber et al., 2023). In the media sector, the printed and electronic press, radio, and TV stations (public and private) are the mainstays of information production and dissemination. Thereby, the media fulfil important educational duties and political control functions. The latter includes the critical processing and research of information - sometimes contrary to governmental confidentiality interests. Moreover, this task has taken on a new quality in the era of new information channels through social media and mass-produced fake news. The culture subsector includes archives, libraries, and museums as sites for the preservation of information, but also cultural monuments that create identity, such as the Brandenburg Gate. The Reichstag fire of 1933 and the subsequent authoritarian decrees may serve as an example of the danger of instrumentalising the destruction of symbolic buildings.

This division into sectors may suggest that their infrastructure and subsystems work independently. In fact, the sectors are highly interrelated and interact with each other in a wide variety of ways, which will be discussed further below. Notably, digitalisation plays an inevitable role across all sectors but also creates new vectors of attack and potential points of failure.

13.4 Essential Concepts of Critical Infrastructure Protection

This section explains four baseline concepts of CI research that are essential to understanding CI.

13.4.1 CI Hierarchies and System-Of-Systems Approach

The System of Systems concept is used to understand and organise the complex interactions and interdependencies between different sectors and infrastructures in a society. This approach emphasises that sectors, infrastructures, and their components should not be viewed as separate from each other. Instead, the importance and influence of a particular sector or infrastructure varies depending on the underlying architecture of systems and subsystems forming complex interactions and hierarchies (see Fig. 13.2).

The components of the overall CI system are categorised into hierarchical levels that are logically or physically interconnected. Three levels of systems exist:

1. **Sector level:** The top-level covering different sectors such as transportation, energy, healthcare, etc.
2. **Sector infrastructures:** At this level, the specific infrastructures within a sector are considered. For example, rail and road transport are separate infrastructures within the transport sector.

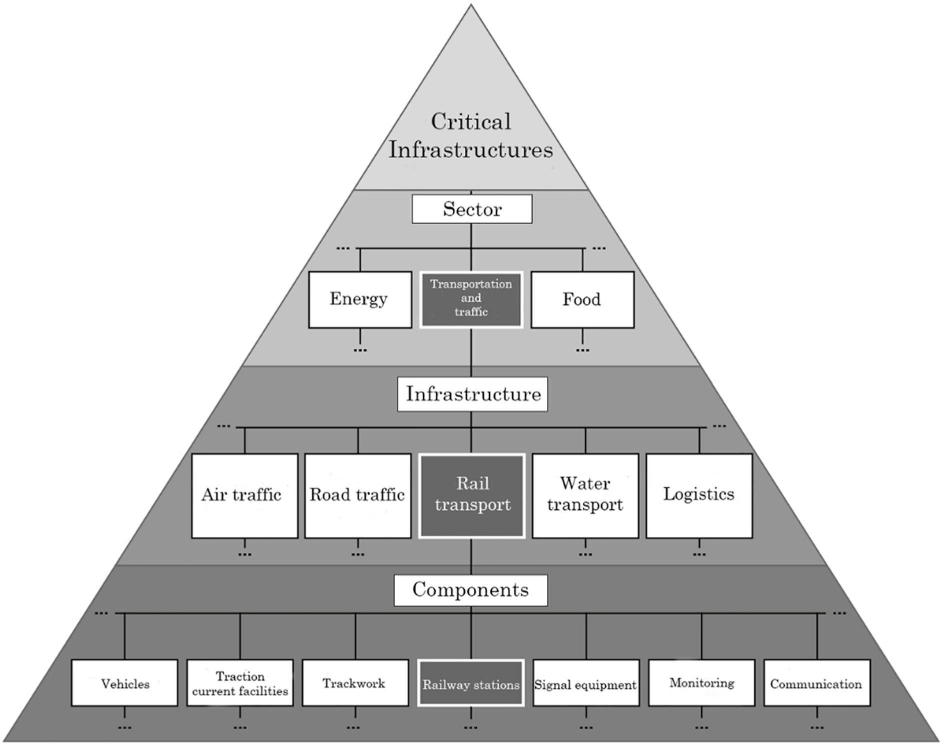

Fig. 13.2 Exemplary CI hierarchy for a railway station as CI component (modified after Lenz (2009, p. 23))

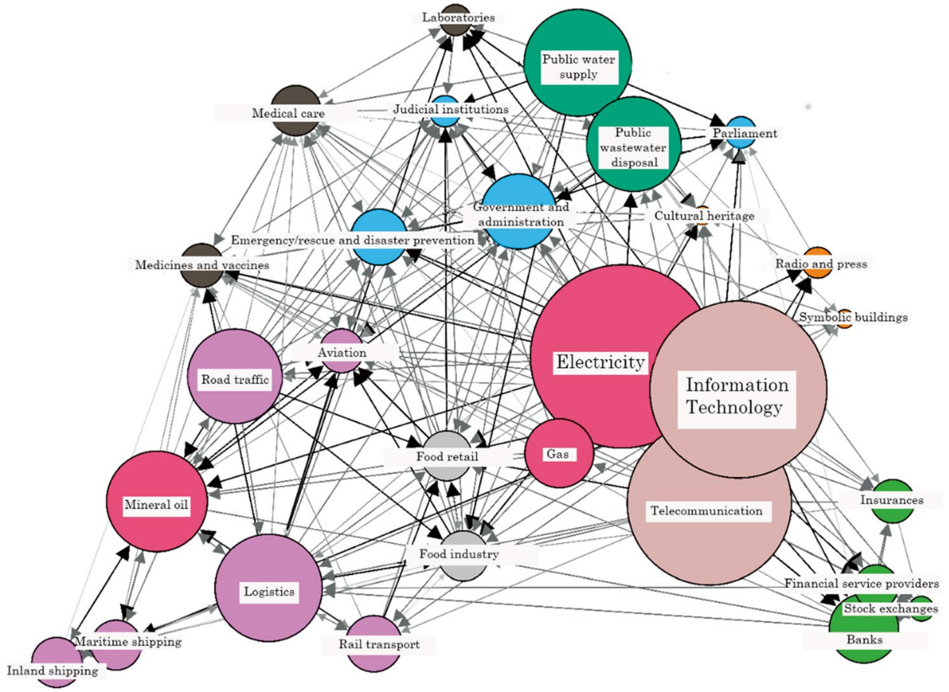

Fig. 13.3 Direct dependencies between CI sector infrastructures, modified after H.C. Schmitt (2023, p. 160)

3. **Components of infrastructures:** This is the lowest level, comprising the concrete elements within an infrastructure, such as rail networks, control systems and human resources.

These hierarchies are necessary to ensure that the critical infrastructures function properly and that the respective sectors are operational. As the sectors do not exist in isolation but interlock to form an overall system, interruptions to services in one infrastructure (sub-)system can **cascade** across other infrastructures. The concept of system of systems illustrates the complexity of the overall CI system, which can never be entirely understood, as some uncertainty always remains about its exact structure and functioning. Nevertheless, it is possible to approximate the complex interdependencies and develop strategies for resilience and security by identifying interactions between systems and subsystems within and across CI sectors (Fig. 13.3).

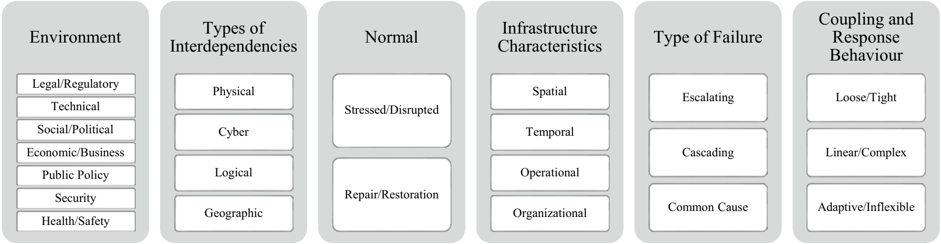

Fig. 13.4 Dimensions for describing infrastructure interdependencies. (own representation after Rinaldi et al. (2001, p. 12))

13.4.2 (Inter-)Dependencies

Dependencies within CI are multifaceted and can have far-reaching effects on various sectors. Structurally analysing these dependencies is crucial in order to identify potential vulnerabilities and develop appropriate resilience measures. This chapter presents and explains the **six dimensions of CI dependency** according to Rinaldi et al. (2001) using examples from various sectors (Fig. 13.4).

These dimensions are essential to consider if modelling or analysis of CI is aimed for:

- First is the **infrastructure environment**, which emphasises the interdependence between infrastructures and their surrounding conditions. Business and economic considerations, influenced by factors such as ownership, regulation, and government policies, shape the operational constraints of infrastructures (see below 13.5.1). Technological advancements, particularly in information technology, contribute to increased interdependencies but also pose security challenges. Legal and regulatory concerns, public policy, and government investments further impact the infrastructure environment. Hence, researchers must consider social and political factors, both nationally and internationally, as integral components of the complex infrastructure environment.
- Second, the four principal **types of interdependencies** in infrastructure systems are physical, cyber, geographic, and logical. Physical interdependencies involve a direct material linkage between two infrastructures, where the state of one depends on the outputs of the other. Cyber interdependencies result from the reliance on information transmitted through computerised systems. Geographic interdependencies occur when local environmental events can simultaneously affect multiple infrastructures due to their spatial proximity. Logical interdependencies involve a state dependence between infrastructures without a direct physical, cyber, or geographic connection, often influenced by human decisions and actions.

- The third is the **state of operation** in infrastructures, viewing it as a continuum with varying behaviours under different conditions. This continuum ranges from optimal design operation to complete failure with a total loss of service. The timing and sequence of events leading to component failures and disruptions lead to varying consequences for users. Understanding infrastructure interdependencies requires identifying continuous dependencies for normal operations, dependencies during stress, and those during service restoration. The complexity of normal operations and repair activities, often involving sequential and parallel functions with uncertainties, needs to be considered for realistic analysis and strategic insights.
- Fourth, key **characteristics of infrastructures** (see above Sect. 13.2) matter in the context of interdependency analyses. Spatial scales range from individual parts to the interconnected web of infrastructures and the environment (Reuter et al., 2020). Geographic scales vary from local to international levels, influencing the level of detail and computational requirements in analyses. Temporal scales, spanning milliseconds to years, affect the relevance of certain infrastructure characteristics in models (Franken et al., 2023). Operational factors, including security and risk considerations, involve procedures, training, backups, and contingency plans. Organisational considerations, such as globalisation, ownership, and regulation, impact infrastructure behaviour and should be evaluated in detailed analyses of interdependencies.
- Fifth, interdependencies can lead to different **types of failures**: cascading, escalating, or common cause. Cascading failures involve disruptions in one infrastructure, triggering failures in others, such as a power outage causing a lack of water supply due to a lack of pumps. **Escalating failures** occur when an existing disruption intensifies another, further delaying recovery. Common cause failures happen when multiple infrastructures are simultaneously disrupted due to a shared factor, like a geographic interdependency where the same landslide affects road, telecommunications, and power lines following the same corridor.
- Lastly, Rinaldi et al. (2001) emphasise the significance of classes of **couplings** among infrastructures and their impact on responses to perturbations. They introduce three primary coupling characteristics: the degree of coupling (tightness or looseness), coupling order (direct or indirect connections), and the linearity or complexity of interactions. Tight coupling implies high dependence, while loose coupling suggests relative independence. The coupling order assesses direct or indirect connections among infrastructures (see Fig. 13.3). The text also distinguishes between linear and complex interactions, highlighting the familiarity of linear sequences and the unexpected nature of complex sequences.

The **response behaviour** – adaptability or inflexibility – of infrastructures under stress depends on factors such as substitutes, contingency plans, institutional learning capacity, regulations, and organisational policies.

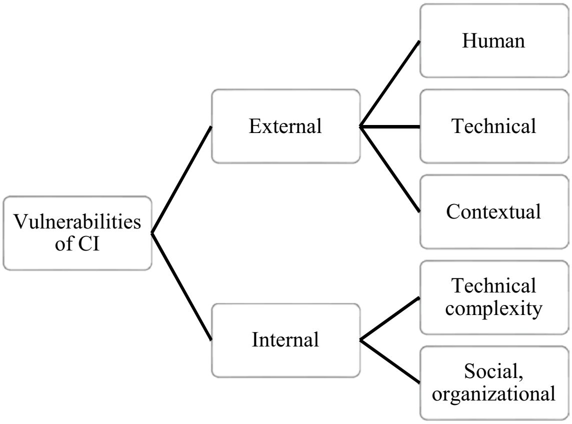

Fig. 13.5 Classification for vulnerabilities of CI (own representation)

13.4.3 Vulnerability of CI and the Vulnerability Paradox

Generally, vulnerability means the susceptibility of an asset. As a concept in **critical infrastructure** research, vulnerability is often used as the opposite term of resilience (see Chapter 14 "*Resilient Critical Infrastructures*"). However, depending on the disciplinary origin, vulnerability has different meanings. Eifert et al. (2018, pp. 22–23) underscore the diverse interpretations across disciplines. In medicine and psychology, vulnerability pertains to an individual's internal **predisposition to disease**. Engineering conceptualises vulnerabilities as **security gaps** often induced either by internal system complexity and dependencies, or external risks like cyber backdoors and physical weaknesses. Geographers view vulnerability through the lens of human **susceptibility to environmental changes**, while development research takes a structural perspective on **disadvantageous context factors** (economic, political, spatial) for societies or any of their sub-components.

Merging these perspectives, vulnerability is the sum of any present condition that raises the impact of a disadvantageous event. As these conditions can dynamically shift over time, vulnerability should not be regarded as a static state (Vries, 2011). As an overview, Fig. 13.5 displays a classification system of CI vulnerabilities.

The vulnerability paradox illustrates the social component of the concept. The following was already established in the German CI strategy:

> To the extent that a country is less susceptible to disruption in its services, the greater the impact of any disruption. (Federal Ministry of the Interior, 2009, p. 8) [translated by the authors]

While, at first sight, it might seem counter-intuitive, the **vulnerability paradox** makes a case for why more robust CI must not necessarily lead to more security. Because, as a social process of perceiving complete security for CI assets sets in, preventive measures and technical, social, and psychological preparedness deteriorate. For example, storing batteries or electric generators for power outages is more likely to be perceived as needless in contexts where outages virtually never occur. If an outage occurs, however, the impacts will be more intense than in contexts of irregular access to electric power, where individual preparation of fallbacks is common. To overcome this situation of reliability leading to unpreparedness, the German government advocates a shift from the existing security mindset to embrace a **risk culture**. This cultural shift underscores transparent risk communication involving the state, businesses, citizens, and the public. Collaboration among all pertinent stakeholders is emphasised for preventing and managing incidents. Additionally, the CI strategy stresses the importance of increased operator commitment and improved self-protection and self-help capabilities for individuals and facilities affected by disruptions.

13.4.4 Criticality

As part of the very notion of CI, criticality is an essential concept for CI-related research. While early approaches to assign criticality were mere factual, descriptive enumerations of vital infrastructure as catalogues or inventories, today, it is more common to interpret criticality as a relative measure. The German CI strategy falls within the latter, describing criticality as a

> relative measure of the importance of an infrastructure in relation to the consequences that a disruption or functional failure has for the security of supply of important goods and services to society. (Federal Ministry of the Interior, 2009, p. 5) [translated by the authors]

Lukitsch et al. (2018) identify three principal directions in the use of criticality concepts that researchers of all disciplines in the field should be aware of:

The first important aspect involves a distinction between **deficiency-oriented and capacity-oriented approaches**. While many CI studies focus on the vulnerabilities and weak points of technical infrastructures, others emphasise the constructive capacities of critical infrastructure, considering its role in providing vital services even during emergencies. In short: Is criticality the negative outcome of the non-functioning of a crisis or the positive coping capacity of an infrastructure during crises?

The second dimension distinguishes **function-oriented approaches**, highlighting the significance of individual components in contributing to infrastructures' overall function. This perspective assesses criticality in relation to a given or desired function, with distinctions between **systems-based and consequence-based** assessments. In short: Is the perspective of the research to identify the bottom-up role of single components or the top-down view of the designated provision of service?

The third direction for research, termed the **pragmatic approach**, takes a meta-perspective to analyse how criticality is constructed within discourses – somewhat like securitisation – ascribing infrastructures as critical through speech acts or practice. According to Lukitsch et al. (2018), analysing the **criticalisation** of elements within a discourse, exploring the complex interplay of actors, context, and audience in shaping perceptions of criticality may reveal problem conflation, problem inflation, or over-simplification of reactions. This is supported by the general acceptance of expanding the inclusion of systems within the critical category rather than reversing such designations. This observation reflects a tendency that potentially contributes to the continuous broadening scope of CI in practice. In short: When, through whom, and under which circumstances are infrastructures successfully assigned to be critical?

13.5 Actors and Responsibilities

Due to their spatial spread, the diverse functions they fulfil, and the complex installation, repair, and maintenance processes, there are a large number of actors – individuals and collective entities – for critical infrastructures. In Germany, the private sector dominates the CI landscape (13.5.1). In addition, there are public institutions at all conceivable levels that are responsible for the regulation of CI (13.5.2). In addition, civil society organisations (13.5.3), which have formed around the topic of CI, also perform monitoring and advisory functions outside the economic and public sectors. These three groups of actors will be discussed in more detail below.

13.5.1 Providers, Operators, and Suppliers

In Germany, around 1600 companies fall within the currently effective CI thresholds of the *IT Security Act 2.0* (*IT-SiG 2.0*). At around 80 percent, the large majority of German CI is in the hands of private companies. This proportion does vary in other countries, as there are few countries that have complete **privatisation** – outside of the state and administration sector, which by definition cannot be privatised – or entire **state responsibility** of the basic service provision (Schneider et al., 2005). Instead, the privatisation rate of infrastructures is gradual, differs depending on the context, and changes over time.

Private CI actors can be roughly classified into three roles:

First, there are the **providers**, i.e. the companies that have committed to providing a service to recipients. For example, these can be large electricity suppliers, local waterworks, or telecommunications giants. Typically, they are legal owners of the infrastructure and responsible for the strategic and overall management of the assets. Sometimes, providers enter into direct contracts with consumers, while other times, they provide their services to other, smaller providers, who in turn make contracts with end consumers. For example, a so-called Tier-1 Internet Service Provider (ISP) can primarily benefit from the transit fees for data paid by the regional Tier-2 ISPs, whereby the latter become customers themselves. On the other hand, in relation to individual end customers, Tier-2 providers are then providers of the services. Companies that fulfil this role are generally regulated by CI legislation because they meet the predefined thresholds (supply thresholds, company size, etc.) (Fekete, 2011).

CI **operators** are entities or individuals involved in the day-to-day operations and maintenance of critical infrastructure assets. They are responsible for ensuring the continuous and secure functioning of these assets. As such, operators play a more hands-on role in daily managing, maintaining, and protecting critical infrastructure. Frequently, providers also operate their infrastructures, but they may also employ or contract with CI operators. For example, (long-distance) transmission system operators in the electricity sector maintain their own control centres and repair resources. On the other hand, the repair and maintenance of local fibre optic cables are often outsourced to subcontractors located in close proximity to the damages and cables. As a result, many subcontractors are not subject to CI regulation despite their activities at CI. The reason for this is that they do not meet the thresholds for company size or utility services.

Nevertheless, the role of suppliers in the context of CI is of crucial importance. The definition of suppliers can be extensive, as it includes not only direct material or product suppliers for CI systems but also the entire supply chain from raw material extraction (primary sector), production (secondary sector), and services related to CI (tertiary sector). Increasingly, states make efforts to include these actors along these supply chains and economic networks in the regulation and dependency analyses. The integration of supply chain actors from the primary and secondary sectors plays a key role, as it is intended to ensure the smooth supply of materials.

An example of the primary sector would be coal mining, which ensures the availability of fossil fuels for power plants and industrial production. The secondary sector would include, for example, the production of fibre-optic cables, which supply telecommunications companies with the hardware they need to perform their tasks. The tertiary sector in the CI context is particularly diverse and includes IT services, customer acquisition, and consulting services, such as surveying services, construction law filing, and the provision of land adjacent to railroad lines and roads.

Recently, a particularly important aspect is the qualification of personnel, especially in the education sector. The availability of well-trained personnel is crucial for the proper operation of CI. However, there is an acute shortage of trained personnel in almost every CI sector due to changing demographics and a general lack of skilled workers. Training and education services as a supplier of specialist personnel thus also serve to ensure the continuity and security of CI.

Considering the motivation of economic players in critical infrastructures sheds light on their necessity and the potential areas of tension that arise from inherent corporate objectives. This is because companies primarily pursue the main objective of profitability, which is in conflict with security requirements to safeguard a reliable supply and other broader motives such as **environmental protection** or **sustainable development**. This challenge can have far-reaching consequences for the security of critical infrastructures. Indeed, companies have the intrinsic motivation to increase the security of a service in order to retain customers. However, if situations of exclusive supply (monopolies) occur, this argument is invalid. In addition, security requirements can extend well beyond the economically advantageous solution if particularly high-value assets are affected or scenarios other than every day, minor outages are assumed. If governments nevertheless want to ensure the performance of CI companies, demanding a higher level of security through regulation is an option. These are intended to ensure that companies invest appropriately in security measures. Reporting, auditing, and sanctioning procedures ensure that companies do not neglect these measures. Therefore, it makes sense to focus on the public actors next.

13.5.2 State and Public Authorities

In the following, the public stakeholders in CI protection are discussed. As a vast subject area, CI regulation is characterised by multi-level governance. Therefore, the various actors and their responsibilities are explained below, from the global to the individual level.

- **International level**: As explained earlier, there is no single global authority to enforce international treaties. Hence, there is no unified global CI protection regulation. However, certain security regulations in specific sectors are often agreed upon within the United Nations Specialized Agencies framework. For example, the International Telecommunications Union (ITU) establishes international communication standards to ensure the compatibility of cross-border data traffic. Another example is maritime shipping, regulated by the International Maritime Organisation. However, institutions at this level generally have no influence on national regulations as long as states are not members of the international organisation.
- **Regional level** (European Union): In Europe, by contrast, the EU is an association of states that is able to pass binding legislation for all member states. Usually, this is achieved by EU directives, for which the specific implementation and formulation through legislation is the responsibility of the national legislator within a set time frame. On the one hand, this two-stage procedure – first on regional, then on national level – slows down implementation processes. On the other hand, it allows consideration to be given to national differences. EU directives should be regarded as the minimum standard for national implementation and can indeed be exceeded in terms of their strictness or level of detail in the member states implementing respective legal acts. The EU Resiliency of Critical Entities (EU REC) EU 2022/2557 and the Network and Information Security 2 Directive (NIS2) EU 2022/2555 are notable directives adopted at the EU level and currently being implemented. While the former primarily addresses physical protection, NIS2 deals with the protection of CI in cyberspace.
- **National level** (Germany): This dichotomy in the regulation of physical and cyber threats is also reflected in the German CI protection architecture. The Ministry of

the Interior is the nationally responsible authority and has two subordinate agencies, the Federal Office of Civil Protection and Disaster Assistance (BBK) and the Federal Office for Information Security, each covering these fields. In addition, the Federal Agency for Technical Relief, a volunteer civil protection organisation, is also subordinate to the Federal Ministry of the Interior. The federal government is generally tasked with protecting the population from war-related risks, called civil protection. However, as disaster relief is a matter for the federal states, the BBK primarily has a supporting role. With around 500 employees, the authority has further responsibilities for warning infrastructures, protective construction (shelters), public health, and cultural property protection and thus only for certain CI sectors. The CI Umbrella Acts (KRITISDg), which implements the latest EU regulations, will turn the BBK into the central point of contact for CI companies. However, not every regulated sector and operator that falls within CI thresholds is directly overseen by the BMI. Apart from compliance with the IT Security Act (ITSiG 2.0), certain operators remain subject to sector-specific regulations enforced by other entities such as the BNetzA (Federal Network Agency of the Federal Ministry of Economic Affairs and Climate Action), BaFin (Federal Financial Supervisory Authority of the Federal Ministry of Finance), and various others.

- **Federal state level** (German federal states): In principle, the German federal states (“Bundesländer”) have the right to legislate (Art. 70 GG), and the national government is only responsible for topical areas within the list of exceptions in Art. 73 (exclusive legislation) or with shared responsibility in Art. 72 GG (concurrent legislation). For this reason, some CI sectors in Germany are regulated at the federal level (e.g. nuclear energy, postal services, telecommunications), while others are regulated by both levels (e.g. food, coastal shipping, waste management). However, there are close to no exclusive federal-state responsibilities for any sector, as they are either mentioned in Art. 73 or 72 GG. The only exception to this is the administrative sector of the federal states. For example, disaster relief is part of general threat prevention and, as such, the responsibility of the federal states, not the central state. Therefore, large parts of the crisis response that may result from large-scale CI outages lie in the hands of German federal states. For example, rescue services and firefighting are regulated at the substate level. Legal reforms like the KRITISDg, while implementing EU regulations, also aim to harmonise CI protection efforts on the federal level.
- **Municipal**: The responsibility of municipalities for CI also varies between the federal states, which causes additional complexities. In general, municipalities are often the owners of certain infrastructures; e.g. the water supply in Germany is usually municipal. They also fulfil many of the local-level administrative tasks. These include planning approval procedures and developing emergency plans for disaster control. These plans then incorporate locally available resources from fire brigades, hospitals, and private rescue organisations and need to be updated regularly.

- **Individual**: Individuals are also active players, both as beneficiaries of CI services and as those potentially affected by their failure. The sense of responsibility for one's own security varies greatly depending on the risk culture (Reuter et al., 2019). Since a state cannot respond sufficiently to all individual needs due to privacy principles, there are, for example, general recommendations and guidelines for stockpiling food and items that are practical in times of large-scale CI outages. Furthermore, warning apps that provide direct warnings with enhanced and personalised messages offer a low-threshold option for individual action. Consequently, individuals can also contribute to the resilience of society as a whole (see Chapter 14 "*Resilient Critical Infrastructures*").

13.5.3 Civil Society and Public–Private-Partnerships

Besides clearly distinctive public or private actors, hybrid and civil society actors have evolved recently. On the one hand, **public–private partnerships** (PPP) are formed to coordinate regulative efforts and economic needs. On the other hand, **civil society** actors fulfil a corrective function.

Exemplary for a PPP, the **UP KRITIS** initiative in Germany fosters collaboration between private enterprises and government entities to protect critical infrastructure. Open to organisations operating in Germany's critical sectors, the initiative involves critical infrastructure operators, associations, recognised single points of contact (SPOCs), and government authorities. Only excluding the state and administration CI sector, UP KRITIS aims to enhance the resilience of critical infrastructure in broad, but also in the sectors and sub-sectors. To enable a level of detail, participants can contribute by joining working groups that focus on internal collaboration within industries and addressing broader issues across sectors. Information exchange in these fora includes, for example, the usage of shared components, common vulnerabilities, experiences with outages, crisis management best practices, as well as broader issues that lead to aggregate risks beyond individual providers or operators.

On the civil society side, there are several initiatives dedicated to the topic of CI. The CI working group (**AG KRITIS**) emerged from the Chaos Computer Club (CCC) and pools CI experts who work primarily on IT issues. The association explicitly sets itself apart from industry associations and public players. The idea of founding a cyber relief organisation, which would be modelled after the German Federal Agency for Technical Relief, is being promoted there (AG KRITIS, 2022). The openKRITIS website also operates as an independent platform, where current CI regulations at national and regional levels are comprehensively analysed in a generally understandable way as a reference guide (Weissmann, 2023).

13.6 Conclusions

Critical infrastructures provide societies with essential goods and services. As digitalisation progresses, information and communication technologies play an increasing role within these entities, and large-scale outages in many of the ten German CI sectors revealed the increasing vulnerabilities stemming from dependencies on electricity and connectivity. While the CI concept is widely used in recent public debates, some inconsistencies require nuanced attention from students and researchers of CI. To enable a coherent analysis of CI, this chapter focuses on secure critical infrastructures and provided an overview of the central characteristics of infrastructures and important concepts of hierarchy, (inter-)dependency, criticality, and vulnerability. Finally, to map out the multi-actor landscape within CI, the private, public, hybrid and civil-society stakeholders mainly shaping CI policies and discourses were introduced. With a more practical approach to CI protection, the subsequent chapter will focus on resiliency as the remaining concept of CI research.

13.7 Exercises

Exercise 13-1: Name typical components of a definition of critical infrastructures.

Exercise 13-2: Describe the characteristics of infrastructures according to Leigh Star and give examples.

Exercise 13-3: Explain types of interactions between infrastructures and name examples of interacting infrastructures or subsystems from four different sectors. What part do electrification and digitalisation of critical infrastructures play?

Exercise 13-4: Discuss: In which way can the German CI regulation architecture be regarded as a multi-level governance field? Name relevant actors for at least three levels.

Exercise 13-5: Are private or public actors the better-suited entities for protecting critical infrastructures? Discuss and justify your opinion.

References

Recommended Readings

Star, S. L. (1999). The Ethnography of Infrastructure. American Behavioral Scientist, 43(3), 377–391. https://doi.org/10.1177/00027649921955326

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). *Identifying, understanding, and analyzing critical infrastructure interdependencies*. IEEE Control Systems Magazine, 21(6), 11–25. https://doi.org/10.1109/37.969131

Engels, J. I. (Ed.). (2018). *Key Concepts for Critical Infrastructure Research*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-22920-7

Krings, S. (Ed.). (2020). *10 Jahre „KRITIS-Strategie": Einblicke in die Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen*. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Also, note the annual ring lecture *"Secure Critical Infrastructures"* in hybrid format at TU Darmstadt.

Bibliography

AG KRITIS. (2022). *Das Cyber-Hilfswerk: Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen* (Version 1.1). AG KRITIS. https://ag.kritis.info/chw-konzept/

Bendiek, A., & Schulze, M. (2021). *Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW* (SWP Research Paper 11/2021). Stiftung Wissenschaft und Politik (SWP). https://doi.org/10.18449/2021RP11

Blankenship, B., & Urpelainen, J. (2020). Electric Shock: The 2012 India Blackout and Public Confidence in Politicians. *Review of Policy Research*, *37*(4), 464–490. https://doi.org/10.1111/ropr.12380

BSI. (2023). *What are Critical Infrastructures?* https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html

Bueger, C., Liebetrau, T., & Franken, J. (2022). *Security threats to undersea communications cables and infrastructure – consequences for the EU*. European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557

Collier, S. J., & Lakhoff, A. (2008). The vulnerability of vital systems: How'critical infrastructure'became a security problem. In *Securing "the Homeland": Critical Infrastructure, Risk, and (In)Security* (pp. 17–39). Routledge.

Cyber Peace Institute. (2022a). Case Study Viasat. *Cyber Conflicts*. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat6

Cyber Peace Institute. (2022b, September 30). Cyber Incident Tracer: Health. *Cyber Incident Tracer*. https://cit.cyberpeaceinstitute.org/explore

Davenport, T. (2018). The High Seas Freedom to Lay Submarine Cables and the Protection of the Marine Environment: Challenges in High Seas Governance. *AJIL Unbound*, *112*, 139–143. https://doi.org/10.1017/aju.2018.48

Eifert, S., Knauf, A., & Thiessen, N. (2018). Vulnerability. In J. I. Engels (Ed.), *Key Concepts for Critical Infrastructure Research* (pp. 21–29). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-22920-7_3

EU-Directive 2022/2557, Pub. L. No. 2022/2557 (2022).

Federal Ministry of the Interior. (2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*. Referat KM 4.

Fekete, A. (2011). Common criteria for the assessment of critical infrastructures. *International Journal of Disaster Risk Science*, *2*(1), 15–24. https://doi.org/10.1007/s13753-011-0002-y

Franken, J. (2022). Seekabel als Maritime Kritische Infrastruktur. In H. Schilling (Ed.), *Dreizack 21: Von historischen bis zukünftigen Herausforderungen im maritimen Raum* (pp. 22–25).

Franken, J., Reinhold, T., Reichert, L., & Reuter, C. (2022). The Digital Divide in State Vulnerability to Submarine Communications Cable Failure. *International Journal of Critical Infrastructure Protection*. https://doi.org/10.1016/j.ijcip.2022.100522

Franken, J., Zivkovic, M., Thiessen, N., Engels, J. I., & Reuter, C. (2023). Das Netz hat Geschichte: Historisch-technische Analyse der kritischen Infrastrukturen in der Region Rhein/Main (accepted). *Lecture Notes in Informatics (LNI) - Proceedings*, *337*, 1563–1573. https://nextcloud.gi.de/s/onnyxKSQoFHdqar

Fraunhofer IAIS. (2019). *Critical Infrastructure*. CIPedia. https://websites.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure#European_Definitions

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A Review of Cybersecurity Incidents in the Water Sector. *Journal of Environmental Engineering*, *146*(5), 03120003. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686

ITU. (2008). *Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts*. Study Group Q.22/1, ITU-D Secretariat.

Jones, A., & Khan, O. (2021). Surviving NotPetya: Global Supply Chains in the Era of the Cyber Weapon. In *Cyber Security And Supply Chain Management: Risks, Challenges, And Solutions* (pp. 133–146).

Klinger, C., Mehdianpour, M., Klingbeil, D., Bettge, D., Häcker, R., & Baer, W. (2011). Failure analysis on collapsed towers of overhead electrical lines in the region Münsterland (Germany) 2005. *Engineering Failure Analysis*, *18*(7), 1873–1883. https://doi.org/10.1016/j.engfailanal.2011.07.004

Kourtis, I. M., & Tsihrintzis, V. A. (2021). Adaptation of urban drainage networks to climate change: A review. *Science of The Total Environment*, *771*, 145431. https://doi.org/10.1016/j.scitotenv.2021.145431

Kuntke, F., Linsner, S., Steinbrink, E., Franken, J., & Reuter, C. (2022). Resilience in Agriculture: Communication and Energy Infrastructure Dependencies of German Farmers. *International Journal of Disaster Risk Science (IJDRS)*.

Kuntke, F., Romanenko, V., Linsner, S., Steinbrink, E., & Reuter, C. (2022). LoRaWAN Security Issues and Mitigation Options by the Example of Agricultural IoT Scenarios. *Transactions on Emerging Telecommunications Technologies (ETT)*.

Lenz, S. (2009). *Vulnerabilität Kritischer Infrastrukturen*. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. https://repository.publisso.de/resource/frl:6401770/data

Linsner, S., Kuntke, F., Steinbrink, E., Franken, J., & Reuter, C. (2021). The Role of Privacy in Digitalization – Analyzing Perspectives of German Farmers. *Proceedings on Privacy Enhancing Technologies*, *2021*(3), 334–350. https://doi.org/10.2478/popets-2021-0050

Luktisch, C., Müller, K., & Stahlhut, M. (2018). Criticality. In J. I. Engels (Ed.), *Key Concepts for Critical Infrastructure Research* (pp. 11–20). Springer.

McLaughlin, R., Paige, T. P., & Guilfoyle, D. (2022). Submarine Communication Cables and the Law of Armed Conflict: Some Enduring Uncertainties, and Some Proposals, as to Characterization. *Journal of Conflict and Security Law*, *27*(3), 297–338. https://doi.org/10.1093/jcsl/krac014

Mitchell, T. (2015). The resources of economics: Making the 1973 oil crisis. In *The Limits of Performativity* (pp. 50–65). Routledge.

Mottaleb, K. A., Kruseman, G., & Snapp, S. (2022). Potential impacts of Ukraine-Russia armed conflict on global wheat food security: A quantitative exploration. *Global Food Security*, *35*, 100659. https://doi.org/10.1016/j.gfs.2022.100659

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations* (Revision 5 800–53; NIST Special Publication). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Nola, M. F. D., Escapa, M., & Ansah, J. P. (2018). Modelling solid waste management solutions: The case of Campania, Italy. *Waste Management*, *78*, 717–729. https://doi.org/10.1016/j.wasman.2018.06.006

Ramos, K. G., Rocha, I. C. N., Cedeño, T. D. D., Dos Santos Costa, A. C., Ahmad, S., Essar, M. Y., & Tsagkaris, C. (2021). Suez Canal blockage and its global impact on healthcare amidst the COVID-19 pandemic. *International Maritime Health*, *72*(2), 145–146. https://doi.org/10.5603/IMH.2021.0026

Reuter, C., Haunschild, J., Hollick, M., Mühlhäuser, M., Vogt, J., & Kreutzer, M. (2020). Towards Secure Urban Infrastructures: Cyber Security Challenges to Information and Communication Technology in Smart Cities. In C. Hansen, A. Nürnberger, & B. Preim (Eds.), *Mensch und Computer 2020—Workshopband* (pp. 1–7). Gesellschaft für Informatik e.V. https://doi.org/10.18420/muc2020-ws117-408

Reuter, C., Kaufhold, M.-A., Schmid, S., Spielhofer, T., & Hahne, A. S. (2019). The Impact of Risk Cultures: Citizens' Perception of Social Media Use in Emergencies across Europe. *Technological Forecasting and Social Change (TFSC)*, *148*(119724), 1–17. https://doi.org/10.1016/j.techfore.2019.119724

Reuters. (2021). *Allianz-Studie—Suez-Blockade kostet pro Woche bis zu 10 Mrd Dollar*. Reuters. https://www.reuters.com/article/handel-suez-kosten-idDEKBN2BI1PB

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25. https://doi.org/10.1109/37.969131

Schmitt, H. C. (2023). *Was heißt hier eigentlich ‚kritisch'? Entwicklung einer Evidenzgrundlage zum Umgang mit kritischen Infrastrukturen in der Raumordnung* [Technische Universität Dortmund]. https://doi.org/10.17877/DE290R-22039

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (M. N. Schmitt, Ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524

Schneider, V., Fink, S., & Tenbücken, M. (2005). Buying Out the State: A Comparative Perspective on the Privatization of Infrastructures. *Comparative Political Studies*, *38*(6), 704–727. https://doi.org/10.1177/0010414005274847

Speidel, U. (2022). The Hunga Tonga Hunga Ha'apai Eruption – A Postmortem: What Happened to Tonga's Internet in January 2022, and What Lessons Are There to Be Learned? *Proceedings of the 17th Asian Internet Engineering Conference*, 70–78. https://doi.org/10.1145/3570748.3570759

Star, S. L. (1999). The Ethnography of Infrastructure. *American Behavioral Scientist*, *43*(3), 377–391. https://doi.org/10.1177/00027649921955326

Star, S. L., & Ruhleder, K. (1996). Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. Information Systems Research, 7(1), 111–134. https://doi.org/10.1287/isre.7.1.111

UNISDR. (2009). 2009 UNISDR Terminology on Disaster Risk Reduction. *International Strategy for Disaster Reduction (ISDR).*

Vries, D. H. de. (2011). Temporal vulnerability in hazardscapes: Flood memory-networks and referentiality along the North Carolina Neuse River (USA). *Global Environmental Change*, *21*(1), 154–164. https://doi.org/10.1016/j.gloenvcha.2010.09.006

Weber, V., Pericàs Riera, M., & Laumann, E. (2023). *Mapping the World's Critical Infrastructure Sectors* (DGAP Policy Brief). German Council on Foreign Relations. https://dgap.org/en/research/publications/mapping-worlds-critical-infrastructure-sectors

Weissmann, P. (2023, November 16). *OpenKRITIS Das unabhängige Nachschlagewerk für KRITIS-Betreiber und Kritische Infrastrukturen.* https://www.openkritis.de/