"DEAR NEIGHBOURS ..." A COMPARATIVE EXPLORATION OF APPROACHES TO MANAGING RISKS RELATED TO HAZARDOUS INCIDENTS AND CRITICAL INFRASTRUCTURE OUTAGES

Susanne Krings

With 1 figure and 2 tables
Received 8 March 2017 · Accepted 9 November 2017

Summary: This paper explores the management of two types of risks which derive from the disruption of normal operations in technical installations: one is related to hazardous incidents, i.e. failures during the course of which substances rated as hazardous are emitted into the environment; the other is related to outages of critical infrastructures, which involve the unavailability of goods and services taken to be essential. Both risks are objects of political debate and administrative action in Germany. The practice of distributing informative brochures in the neighbourhood of a power plant serves as a starting point for a comparative exploration of approaches to handling risks associated with sites prone to hazardous incidents and with critical infrastructures. Starting from here, the paper addresses characteristic features of the practices applied in accordance with the two risk management approaches. The empirical basis comprises a variety of instruments, some more and some less binding, which seek to shape risk management practices, such as laws, recommendations or political strategies. The paper first addresses the federal level (and the influence of the European Union) before the scope is widened to include the other administrative levels, i.e. states and municipalities. The exploration first considers the ways used to designate the relevant facilities. While hazardous sites are bindingly identified at all levels on the basis of a common legal framework, determination of critical infrastructures is considered a context-dependent undertaking and is only partially regulated. Further, it is ascertained that the approaches divergently conceptualize the relations between the 'source of risk' and who or what is 'at risk'. Physical distance (or proximity) is treated as paramount with regard to risks related hazardous incidents, whereas a functional relationship, i.e. a degree of dependency, is taken to be decisive in the context of critical infrastructures. Finally, the two approaches are shown to exhibit diverging attitudes to providing site-specific information to the public. The hazardousness of a site is designated to be public information but its criticality, on the contrary, is to remain classified. As expounded in the last section, these conceptional differences may lead to practical difficulties in civil protection operations.

Zusammenfassung: Der vorliegende Beitrag widmet sich zwei unterschiedlichen Risiken, die mit Störungen des normalen Betriebsablaufs technischer Einrichtungen in Verbindung stehen: zum einen geht es um Störfalle, in deren Verlauf als gefährlich eingestufte Substanzen in die Umwelt gelangen, zum anderen um Ausfälle Kritischer Infrastrukturen, bei denen es zur Unterbrechung der Versorgung mit Gütern und Dienstleistungen kommt, die als besonders wichtig bewertet werden. Beide Risiken sind Gegenstand politischer Auseinandersetzung und administrativen Handelns in Deutschland. Der Versand von Informationsbroschüren an die Nachbarschaft eines Kraftwerks dient als Ausgangspunkt für eine vergleichende Betrachtung der Herangehensweisen an Risiken im Zusammenhang mit ‚störfallgefährlichen' Anlagen und Kritischen Infrastrukturen. Davon ausgehend werden charakteristische Eigenschaften beider Risikomanagement-Ansätze herausgearbeitet. Als empirische Grundlage dienen Instrumente, die mit unterschiedlich hoher Verbindlichkeit die risikobezogenen Handlungen anderer anleiten – von gesetzlichen Regelungen, über Handlungsempfehlungen bis zu politischen Strategiepapieren. Anfangs steht die Bundesebene (und der Einfluss der Europäischen Union) im Mittelpunkt der Betrachtung, bevor im letzten Teil des Beitrags der Blick auf die anderen administrativen Ebenen ausgeweitet und Länder und Kommunen in die Betrachtung einbezogen werden. Die Untersuchung wendet sich zunächst den unterschiedlichen Wegen zu, die betreffenden Anlagen zu bestimmen. Während ‚störfallgefährliche' Anlagen auf Basis gesetzlicher Bestimmungen über alle Ebenen hinweg gleichermaßen und verbindlich als solche identifiziert werden, gilt die Identifizierung Kritischer Infrastrukturen als kontextabhängiges Unterfangen und ist nur teilweise geregelt. Darüber hinaus wird aufgedeckt, dass die beiden Ansätze das Verhältnis der Gefahrenquelle zu den Schutzgütern auf unterschiedliche Weise konzeptualisiert. Distanz (bzw. Nähe) im physischen Raum wird als maßgeblicher Einflussfaktor im Kontext von Störfallrisiken behandelt, während eine funktionale Beziehung bzw. ein Abhängigkeitsverhältnis im Zusammenhang mit dem Risiko des Ausfalls Kritischer Infrastrukturen als besonders wichtig erachtet wird. Schließlich sind beide Ansätze von einer gegensätzlichen Haltung zur Information der Öffentlichkeit über die Natur der betreffenden Einrichtungen geprägt: Die ‚Störfallgefährlichkeit' einer Anlage ist eine zu veröffentlichende Information, die Kritikalität einer Anlage unterliegt jedoch der Geheimhaltung. Die beschriebenen konzeptionellen Unterschiede können, wie abschließend ausgeführt, praktische Probleme für die Gefahrenabwehr hervorrufen.

Keywords: Critical infrastructure, Germany, hazard, hazardous incident, risk management, social geography

https://doi.org/10.3112/erdkunde.2018.02.03 ISSN 0014-0015 http://www.erdkunde.uni-bonn.de

1 Introduction

The history of this paper started with a brochure addressed to the 'dear neighbours' of a power plant. A simple online search revealed it to have numerous counterparts addressed to the neighbours of other facilities (e.g. Kraftwerk Wilhelmshaven 2016; EnBW 2016) all having something in common: they are licensed according to the German *Hazardous Incident Ordinance* (*Störfall-Verordnung*, 12. BImSchV). This ordinance obliges operators to share information on the nature of their facilities with the public and they conform (i.a.) by publishing such brochures (12. BImSchV, sect. 11; cf. BMU 2004, 67–75). Following the praxeological approach Müller-Mahn and Everts (2013) propose introducing their concept of 'riskscape', risk management – understood as a set of practices that systematically address risk – systematically (re)produces the risk it is geared towards. The 12. BImSchV, in that line of reasoning, (re)produces the abstract risk of a **hazardous incident (HI)** and, by making others act in a certain way, contributes to the (re)production of the risk of an incident occurring at a specific facility. The assumptions on the risks associated with 'hazardous facilities' incorporated in the ordinance are echoed in the brochures, which leads to the (re)production of risks that share a set of coherent features. As these practices have a spatial dimension, they constantly (re)produce the spatiality of the risks they address, which leads to the emergence of characteristic riskscapes Müller-Mahn and Everts (2013, 26) refer to as "socio-spatial images of risk".

A power plant might well be at the centre of practices concerned with another kind of risk: it is an element of the electricity supply system, a sub-sector of what is referred to as **critical infrastructures (CI)** specified in the German *National Strategy for Critical Infrastructure Protection* (*CIP Strategy,* BMI 2009). Consequently, it seems possible for the same type of facility to be the object of two distinct risk management approaches. Each of these risks "occupies, not just metaphorically, a specific territory" (Müller-Mahn and Everts 2013, 24) so the riskscapes engendered when handling them are likely to "overlap in time and space" (ibid.). As risk management practices geared towards different risks are not necessarily complementary (or at least self-contained) but might well run counter to each other, overlapping riskscapes will reflect these contradictions (ibid., 24 and 35).

With respect to the diversity of riskscapes Müller-Mahn and Everts (2013, 25) draw from an understanding of 'landscape' as corresponding to observers: "It might be the same stretch of land, but what is perceived and actively apprehended depends on the viewpoint or perspective of the observer. It is never one landscape […] but multiple landscapes". Similarly, they make the point that, "there is not one riskscape but multiple riskscapes" (ibid.; with reference to Appadurai 1990). While Müller-Mahn and Everts use the terms 'perspective' and 'viewpoint' interchangeably they will in the following assume specific meanings. Just as the observers of a landscape may look in a particular direction to see a distinct section of their surroundings, it is possible to focus one's attention not on the whole range of possible risks but on one specific type. Hence, a perspective in the context of this paper denotes an orientation towards a specific type of risk. To resume the above example, depending on the perspective a power plant might be recognized as a hazardous site in the 'hazardous incident perspective' (**HI perspective**) or as a CI component in the 'critical infrastructure perspective' (**CI perspective**). Observers looking at a landscape are situated at particular viewpoints from which they perceive what is in sight. Correspondingly, in the context of this paper, a viewpoint characterizes the position from which a risk is conceived of. Due to different viewpoints, even those who adopt the same perspective will conceptualize the respective risks somewhat divergently. Within the HI perspective a facility might, for instance, be regarded as 'hazardous' from the viewpoint of a worried citizens' initiative, however, it might not classify as such from the viewpoint of the relevant inspecting authority implementing the appropriate legal framework. Perspectives and viewpoints necessarily interact and, consequently, both perspectives and viewpoints shape risk management practices and the riskscapes they produce.

The brochure mentioned above indicates that the approaches to handling risks associated with HI differ from the approaches concerning CI. Taking this conjecture as a starting point, this paper seeks to disclose some characteristic features of the two perspectives introduced in section 2, the CI perspective and the HI perspective. As to their common features, firstly, both the hazardousness and the criticality of facilities might go unnoticed as long as everything runs smoothly: they only materialize in a disruptive incident[1]. Secondly, they both point to the ambivalent

[1] Star (1999) gave prominence to the notion that it is an inherent feature of infrastructures only to become visible upon discontinuation of service. On 'the blackout' as an epistemic event cf. Koch (2016).

nature of the facilities in question as they represent different kinds of unintended (and unwelcome) side-effects. These perspectives will primarily be explored from the viewpoint of the German state at federal level – a necessary specification: On the administrative side alone authorities at different levels (from the EU to the local community) contribute by taking a number of different steps, from legislative means to operative emergency management measures. In fact, even the supplement 'at federal level' to a certain degree conceals a more complicated situation: the perspectives are part of different policy areas and different authorities are primarily concerned with the issues. The management of risks related to hazardous incidents is part of environmental policy in the responsibility of the *Ministry for the Environment, Nature Conservation, Building and Nuclear Safety* (*Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit,* BMUB). **Critical infrastructure protection (CIP)** is expressly treated as an inter-ministerial issue, coordinated at the *Ministry of the Interior* (*Bundesministerium des Innern,* BMI).

2 Scope of the paper

The HI perspective focuses on the risks related to HI as defined in the context of the *Hazardous Incident Ordinance* (*Störfall-Verordnung*, 12. BImSchV) of the Federal Immissions Control Act (Bundes-Immissionsschutzgesetz, BImSchG). Putting it simply, those incidents arise from a disruption of normal operation, they involve hazardous substances and threaten to cause death, serious health impairment, health impairment to a large number of people, or damage to the environment, cultural or other material goods to an extent that affects the common good (12. BImSchV, sect. 2). The hazardousness of facilities appeared on the German political agenda in the 1970s. It was about that time that, according to Beck (1986, 27), German society began to increasingly address the side-effects of industrially driven economic development as risks – the transformation into the 'risk society' set in. Its appearance coincides with German geographers turning to the issue. Geipel (1982) used the term 'sperrige Infrastruktur' (initially coined by Weyl 1978; proposed translation: 'noxious facilities', Geipel 1982, 7) to embrace the tensions caused by facilities generally considered to be necessary while at the same time being 'unpopular' with those living in their vicinity.

In retrospect the German *Federal Environmental Agency* (*Umweltbundesamt*, UBA) describes two partially interrelated aspects as typical of environmental policy in the Federal Republic of Germany (FRG) in the 1970s[2]: Firstly, its protagonists were all legal experts and accordingly the instruments applied were mainly legislative; secondly, the approaches were animated by a strong belief in the problem-solving capacity of planning (*Machbarkeits- und Planbarkeitsgläubigkeit*) popular at the time (UBA 2015, 19). Shortly after raising environmental issues and announcing several legislative proposals in a government declaration in 1969 an ad-hoc programme issued in 1970 specified the next steps (Bundestags-Drucksache VI/2710, 7). When in 1971 the more comprehensive government programme was presented the relevant legislative procedures were already under way (ibid.). The FRG became a forerunner in environmental legislation in Europe by passing a number of acts in the following years (Aden 2012, 18; Radkau, 2011, 128) including the above-mentioned BImSchG in 1974 and the 12. BImSchV in 1980. The European directive "on the major-accident hazards of certain industrial activities" (Council Directive 82/501/EEC) adopted in 1982, and the related directives that followed (Council Directives 96/82/EC and 2012/18/EU) have been integrated into the 12. BImSchV.

The CI perspective focuses on risks resulting from outages of infrastructure services. The German federal government's approach to these risks is articulated in the National Strategy for Critical Infrastructure Protection (CIP Strategy) in the context of which CI are defined as "organizational 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 disruption of public safety and security, or other dramatic consequences" (BMI 2009, 4). As the strategy puts it, it is "modern, efficient societies", specifically Germany, one of the "leading industrial and technology-oriented nations", to which the availability of "high-performance and well-functioning infrastructure" (ibid., 3) is a matter of concern. Aradau (2010, 506) describes infrastructures in the context of CIP as becoming "materialized through their capacity for being disrupted and their effects upon the smooth functioning of society".

The starting point of activities labeled as CIP in Germany can be traced back to 1997 (BMI 2008, 7; Lauwe and Riegel 2008, 115). Taking up the issue was at least partly motivated by the publication of the internationally influential final report of the

[2] On environmental policy in the German Democratic Republic cf. Huff (2015).

President's Commission on Critical Infrastructure Protection in the United States (PCCIP 1997; cf. Schulze 2006, 155; Brunner and Suter 2008, 160)[3]. In the first few years, activities in Germany remained at a comparatively low level and attention was predominantly focussed on IT-related issues (Schulze 2006, 155–159); later "the events of 11 September 2001" not only "added urgency to ongoing efforts" but also "as part of the campaign against terrorism, contributed to widening the scope of national activities and intensifying the international dialog" (Brunner and Suter 2008, 160; cf. Schulze 2006, 159 & 206)[4]. Today the federal and state governments subdivide CI into nine sectors: 'energy', 'finance and insurance industry', 'food', 'government and public administration', 'health', 'information technology and telecommunications', 'media and culture', 'transport and traffic' and 'water' (BBK and BSI 2011, cf. also list of sub-sectors). Following the example of the power plant in the introduction, this paper will occasionally refer to the electricity supply system as part of the energy sector. To better understand the relevance of this sub-sector the German parliament commissioned a study on the consequences of a "prolonged and widespread power outage" (Petermann et al. 2011, 5). It concluded that the consequences of this scenario "could at least be akin to a national disaster" (ibid.).

As stated in the "guiding policy concept" of the strategy, the state primarily acts "as a moderator" in CIP and only if required interferes in a "rule-making" manner (BMI 2009, 3): As the infrastructures in question are increasingly owned and run by private companies, "the responsibility for the security, reliability and availability of such infrastructure increasingly passes to the private sector or, at least, becomes a shared responsibility" (ibid., 8). Against this background the "institutionalized, organized co-operation of the state and business and industry within the framework of established security partnerships" (ibid., 8) is declared a requirement. However, the role of legislation in CIP in Germany is multifaceted, as some aspects with relevance for CIP have, in fact, been implemented by legislative means. This, for instance, applies to the directive "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" (Council Directive 2008/114/EC) adopted in the context of the *European Programme for Critical Infrastructure Protection* (Commission of the European Communities 2006, cf. also European Commission 2013). It was integrated into the German *Energy Industry Act* (*Energiewirtschaftsgesetz*, EnWG) in sect. 12g on the "protection of European critical facilities" (my translation). The same act, without making explicit reference to CIP (e.g. by using the appropriate vocabulary), obliges operators i.a. to provide a "secure, reliable and high-performance energy supply grid" (EnWG, sect. 11; my translation; cf. John-Koch 2017, 192). Hence, it may be inferred that legal frameworks regulating infrastructure supply in Germany offer a number of implicit entry points for CIP-related issues (cf. BMI 2009, 3; BMI 2008, 12–13; BMI 2005b, 9)[5].

In summary, while risks related to the hazardousness of facilities have been on the agenda for about forty years, CIP only became the object of political debate about twenty years later. Not only have these policy areas had considerably divergent periods of time to evolve but they have also emerged and unfolded in historically different political contexts. HI became a political topic in the wake of the so-called 'ecological revolution' (Radkau 2011, 124–164) when environmental degradation was increasingly recognized as existentially threatening. Pursuant to the general mentality of the late 1960s and early 1970s (and to the profession of the personnel involved) environmental politics primarily addressed these issues by means of legislation (UBA 2015, 19). CI entered the political stage in the late 1990s. It evolved against the background of progressive privatization of formerly public infrastructure services (BMI 2009, 8) and in a security environment influenced by international terrorism (Brunner and Suter 2008, 160; Schulze 2006, 206). The assumption of the above-mentioned 'shared responsibility' and the understanding of the state as a 'moderator' match the use of legislation in CIP. Whereas a legislative instrument has been playing a central role in the management of risks related to HI from the beginning, there is still no direct equivalent in the policy area of CIP. Consequently, the following analysis with respect to the HI perspec-

[3] However, the government in May 1997 replied to a query from parliament that no equivalent to PCCIP were needed in Germany (Bundestags-Drucksache 13/7753, 10).

[4] IT related aspects and the sub-issue of *Critical Information Infrastructure Protection* have continuously played an important role, cf. BMI (2005a) with BMI (n.d.), BMI (2011a), BMI (2016) and IT-SiG.

[5] Explicit reference to CIP is made in federal legislation on spatial planning (*Raumordnungsgesetz*, ROG), civil protection (*Zivilschutz- und Katastrophenhilfegesetz*, ZSKG) and IT-security (*IT-Sicherheitsgesetz*, IT-SiG). On the use of legislative instruments in CIP in Germany cf. Wiater (2013) and Wiater (2017).

tive will heavily rely on the appropriate legislative act while most of the documents referred to in the context of CIP have no legally binding force.

Finally, it should be noted that a number of acts – the *Sicherstellungsgesetze,* an umbrella term which awkwardly translates as 'acts to guarantee the maintenance of services' – have their roots in the 1960s. These acts were drafted to 'guarantee' basic supplies for the population and the armed forces in times of war (Vossschmidt 2016, 430). They have later been complemented by a number of *Vorsorgegesetze,* best understood as 'contingency laws', which serve as the legal basis for providing supplies in crises without being restricted to wartime situations (ibid., 431). Electricity supply, which this paper mainly refers to, is subject to the *Energiesicherungsgesetz* (EnSiG), a contingency law. The relevance of these acts for CIP in Germany today has not been fully explored yet (cf. Kloepfer 2010, Lauwe 2016). A general overview is given by Vossschmidt (2016, 430–448) and Kloepfer (2015, 196–210).

3 Separate(d) perspectives

As illustrated by the example of the power plant in the introduction the same type of facility might theoretically be relevant to both CI and HI perspectives. Consequently, risk management practices geared towards the two different risks may not only have a bearing on but may even be concerned with the same facilities. This leads to the question to what extent the potential hazardousness of facilities is considered in CIP. Hints can be found both in the classification of CI sectors and in the way the issue is being addressed in the relevant documents. In fact, there are indications that the ties between the two perspectives were much stronger in the past and have only separated relatively recently in the course of the development of CI outages as a distinct type of threat.

From 2004 onwards a classification was used comprising a total of eight sectors – 'hazardous materials' being one of them (cf. BMI 2008, 10). An even earlier version used in BSI (2004, 67) did not contain an equivalent to the 'hazardous materials' sector so its introduction was the result of a revision (cf. Schulze 2006, 132–135; Tab. 1). However, as it was the only one not representing a service sector such as 'energy' or 'health', it rather gave the impression of an adjunct. The *Baseline Protection Concept* (BMI 2005b) does not quote the classification but the issue of 'hazardous facilities' is raised in a number of passages in the text. It sees the obligations operators are put under by the 12. BImSchV as a possible "point of reference" (BMI 2005b, 9) for CIP measures. Additionally, the "release of hazardous substances" is listed as a category of hazards (ibid., 18) with the remark that "the hazardous substances used at a company can be identified by means of an individual register of hazardous substances"[6]. A passage on "risk and crisis communication" even contains the explicit statement that a critical infrastructure might also be a 'hazardous facility' by describing the implications the *absence* of this conjunction would have for management procedures: "For facilities relating to critical infrastructures which are *not* subject to the Ordinance on Major Incidents, the necessary information should be gathered and documented as an essential element of integrated security management" (ibid., 42; my italics; cf. also ibid., 35).

The same classification (with minor changes in wording) can be found in the guidelines for *Risk and Crisis Management* (BMI 2008, 10, cf. Tab. 1), but without any further reference to the 'hazardous materials'. The 'list of threats' in the annex contains the entry "accident involving dangerous goods within the facility or in its immediate vicinity" (ibid., 43) which actually entails that CI elements may simultaneously be hazardous. This point, however, is watered down in the accompanying remarks which describe the sources of the threat as being close by but nonetheless external to the facility: exposure is considered to be an issue "*near* transport routes of hazardous goods" and "*near* facilities in which hazardous goods are used" (ibid.; my italics). In the *CIP Strategy,* a table listing the range of hazards to be addressed contains the category "accidents and emergencies" (BMI 2009, 9), which could have served as a toehold for referring to the risks associated with HI, yet there is no such explanation in the text. The revised classification currently in use, an addendum to the strategy, no longer includes an equivalent to the 'hazardous materials' sector (cf. Tab. 1). The classification is said to be a revision and BBK and BSI (2011) do provide information on some changes, but there is no mention of the deletion of the sector 'hazardous materials'.

Drawing a preliminary conclusion: hazardousness was introduced as a feature of some CI in the earlier version of the sector classification and it was treated as such in the *Baseline Protection Concept* (BMI 2005b). In the following years the sector 'hazardous materi-

[6] The German version indicates that these substances might actually be used *in* the facility in question which would even more explicitly imply the hazardous nature of the CI component (BMI 2005c, 12).

Tab. 1: Lists of critical infrastructure sectors as presented in BSI (2004), BMI (2008) and BBK & BSI (2011)

Critical infrastructures as listed in BSI (2004, 67)*	Critical infrastructure sectors as listed in BMI (2008, 10)	Critical infrastructure sectors as listed in BBK & BSI (2011)**
energy	energy (electricity, oil, natural gas)	energy
telecommunications and information technology	information and communications technology	information technology and telecommunications
transport system	transport	transport and traffic
health care	water and food supply, health care, emergency medical services	health
		water
		food
emergency services		***
financial and insurance systems	banking and finance	finance and insurance industry
public agencies and public administration	government authorities, public administration and the judicial system	government and public administration
	media, major research institutes and cultural assets	media and culture
	hazardous materials (chemical industry and biological substances)	

Notes: The denotations of the sectors are consistent with the original texts but the order of these subdivisions has been altered to better illustrate overlaps and differences between the versions.

* The word 'sector' is not used here.

** Cf. also list of sub-sectors.

*** 'Emergency/rescue services including civil protection' is listed as a sub-sector to the sector 'government and public administration' in this version

als' was excluded from the classification and later publications, such as the guidelines for *Risk and Crisis Management* (BMI 2008), only vaguely imply the possibility that a CI might potentially become the source of a HI. Consequently, risks related to the 'critical' quality of facilities have been established as a type of risk distinct from those related to their hazardousness: the separation of the two perspectives seems to have increasingly materialized over time. Simultaneously, the interrelatedness of the two types of risks in terms of HI threatening CI has to a lesser degree been pointed out in later publications. While the *Baseline Protection Concept* (BMI 2005b) explicitly draws this connection, more recent publications, including the *CIP Strategy* (BMI 2009), do so only very indirectly. HI are now counted among the numerous types of threats for CI following the "all-hazards approach" (BMI 2009, 9).

Regarding links to the CI perspective in documents related to the HI perspective, in the 12. BImSchV (annex VI) the effects a HI might have on infrastructure service play a role in the notification requirements. The operators must report an incident to the authorities when it causes disruptions of phone lines or electricity, gas or water supply exceeding certain thresholds of duration and the number of people affected. Accordingly, facilities prone to HI are seen to be a potential threat to infrastructure supply. Whether or not the 'hazardous facility' in question might also be a CI component is neither implied nor denied. Guidelines for the implementation of the ordinance state that the "security relevant aspects of the energy supply of a facility including the emergency power supply system" have to be part of the operator's security reports (BMU 2004, 14; my translation; cf. 12. BImSchV, sect. 9). They specify that requirements to prevent or contain HI may consider interruption of energy supply and protective measures may include emergency power supply (BMU 2004, 36 & 39; cf. 12. BImSchV, sects. 4–5). So, loss of energy supply is addressed as potentially

causing HI or aggravating the situation during the course of events. In short, some aspects of the CI perspective are taken into account but it is not considered comprehensively.

4 Comparative exploration of the hazardous incident and critical infrastructure perspectives

The practice of systematically informing the neighbours on the hazardous nature of facilities in the HI context and, specifically, its incompatibility with the CI perspective runs like a thread through the following section. Searching for explanations for this initial observation brings to light some basic characteristics of the two perspectives. The empirical material comprises a range of 'meta-practices' which (with different degrees of bindingness and explicitness) seek to systematically shape risk management: legislative acts, regulations, guidelines, recommendations or political strategies. The documents analysed in this section represent the viewpoint of the state at federal level and, where applicable, of the EU, for it strongly influences the proceedings in Germany as a member state.

4.1 Identification of sites

Determining which operators are obliged to take measures to contribute to managing risks related to their sites (e.g. informing the neighbours) would require having identified the facilities which fall into the categories 'hazardous' and 'critical' beforehand. This is the case as concerns facilities under the obligation imposed by the 12. BImSchV (sect. 2): the criteria applied to identify them are concerned with the type and amount of hazardous materials that are present in the facilities as specified in annex I. But, by contrast, separating the critical and the 'uncritical' infrastructures in a comparable way has for long been an unsolved issue (John-Koch 2014, 2017). While in the *CIP Strategy* it becomes clear that it is their *criticality*, the "relative measure of the importance of a given infrastructure in terms of the impact of its disruption or functional failure on the security of supply, i.e. providing society with important goods and services" (BMI 2009, 7), that distinguishes the critical from all other infrastructures, the document lacks instructions as to how it is to be operationalized. The classification of sectors and sub-sectors (BBK and BSI 2011, cf. Tab. 1) serves as a specification but still doesn't allow for the identification of specific facilities. The *Baseline Protection Concept* (BMI 2005b) and the guidelines for *Risk and Crisis Management* (BMI 2008) recommend site-specific measures without being explicit on what sites they should be applied to[7].

Different levels of specificity may be related to the use of regulative means: While a legislative act with a clearly defined scope has for decades been central in the management of risks related to HI, the rather 'modest' use of regulative means in CIP in Germany kept the identification of CI facilities and their operators from becoming a pressing issue for some time. During the implementation of Council Directive 2008/114/EC an identification process has been conducted, but restricted to the energy and transport sectors and explicitly designed to detect "*European* critical infrastructures" (my italics) defined as "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States" (Council Directive 2008/114/EC., art. 2b). The *IT-Security Act* adopted in 2015 contains obligations for the operators of those infrastructures regarded as critical according to the act, so the need to identify the relevant facilities has only recently become more tangible (IT-SiG, art. 1, sect. 8d, para. 2; cf. John-Koch 2014, 4). The appropriate ordinance, the *BSI-Kritisverordnung* (BSI-KritisV), now facilitates identification of CI from the viewpoint of the federal level and in the sectors the IT-SiG applies to by translating the 'relative measure' of criticality into absolute thresholds for this particular purpose.

The restriction to the IT-SiG is necessary as, despite fixing thresholds in the ordinance, generally speaking criticality is still addressed as a determiner to be concretized for the various administrative levels or spatial units (John-Koch 2017; Stolzenburg and Müller 2014)[8]. Thresholds separating the critical from the 'uncritical' sites are seen to vary according to the various levels of description. Hence, efforts to identify CI in various contexts will lead to different sets of sites. By contrast, the understanding of a 'hazardous facility' established by the 12. BImschV is relevant for regulations at other administrative levels: Civil protection laws at state level, for instance, contain obligations to set up 'external emergency plans' at the municipal level for sites subject to the 12. BImSchV (e.g. BHKG, sect. 30). A direct line of reference leads to a congruent notion as to what facilities

[7] On the operationalization of criticality see Fekete (2011).

[8] Guidelines for identifying CI facilities were published after this paper had been accepted (BBK 2017).

shall be considered hazardous across the different levels, from the federal through the state to the municipal. Although the BSI-KritisV in the CI perspective and the 12. BImSchV in the HI perspective similarly serve to identify concrete sites, the ordinances have different 'modes of operation'.

4.2 At risk: a question of proximity or connexity

As specified in sect. 11 of the 12. BImSchV, the operators have to provide information on the plant to all persons and all facilities frequented by customers that could be affected by an incident. Recommendations for the implementation of this section of the ordinance describe "the affected" as "individuals who under normal and adverse circumstances might be present in the hazard zone" (Claus et al. 1999, 11; my translation). The form of address in the brochures mentioned above, 'dear neighbours', gives evidence on how this target group is being identified and it incorporates information on the spatial dimension of the practices employed to manage the risks associated with HI: spatial proximity is obviously considered to make a significant difference[9]. This practice of zoning corresponds to emphasizing a certain aspect of risk: whoever (or whatever) is at risk is primarily defined in terms of *exposure*. Being potentially exposed to the effects of a HI presupposes being close to a facility that might become the source of such an incident – becoming a victim involves being nearby when it happens. A hazardous facility is seen as the source of what November (2004, 276) describes as a "focused risk" characterised as "concentrated on one site".

Turning to the CI perspective, the question of what role exposure plays is more difficult to answer. In fact, had a comparison to the management of risks related to HI not been sought, it is likely that this question would not have been asked in the first place: who or what might generally be affected by an outage in terms of exposure is not being addressed in a comparable way in the documents on CIP[10]. A reasonable explanation relates to the nature of the threat which is at the centre of attention in the CI perspective – the unavailability of a common service. The universal supply of infrastructure services becomes a mixed blessing in the CI perspective (cf. Kaufmann 2010, 107). Most of the CI sectors have a counterpart in the sectors of 'essential public services' (*Daseinsvorsorge*) in Germany (cf. BBSR 2012, 53; Einig 2008, 18)[11]. These services are to be supplied nationwide at an acceptable service level and at affordable prices (BBSR 2012, 31). As concerns electricity supply, the *Energy Industry Act* (EnWG, sect. 36), with few exceptions, requires access for every household[12]. When almost everyone has access to electricity, this, in turn, means that almost everyone is potentially exposed to its failure – the comprehensive provision of service inevitably spreads this risk. Following this argumentation, not mentioning exposure in the documents does not necessarily imply its irrelevance. Indeed, its unquestioned omnipresence may lead to exposure literally *not* making a difference. Rather than being a focused risk a spatially defined group is exposed to, a blackout is better described by what November (2004, 276) terms a "diffuse risk" marked by dispersion.

Instead, more emphasis is put on *vulnerability* in the CI perspective as is clearly expressed in the following: "society's vulnerability has, over the past few years, grown rapidly on account of the increasing extent to which nearly all spheres of life are pervaded with, and dependent on, critical infrastructure" (BMI 2009, 5). The so-called "paradox of vulnerability" (ibid., 10) illustrates the preoccupation with vulnerability in CIP. It describes a decreasing ability to deal with the consequences of service outages *because* they hardly ever occur: "an absolutely fallacious sense of security develops and the impact of an 'against-all-probability' incident [...] will be disproportionately severe". When both outages of infrastructure service and constantly running infrastructures are seen to be enhancing risk, risk management finds itself in a tricky position: as it seems, further improvement of reliability of service might result in aggravating the negative consequences of an increasingly improbable, yet never impossible, disruption. This paradox partially results from the fact that two different vulnerabilities are being addressed: the vulnerability of

[9] As to the localization of hazard zones on the basis of scenarios cf. BMU (2004, 20–22) and SKF (1999); cf. also Hecht (2003, 17).

[10] The picture changes when a scenario-based approach to analysing risk is applied. Manuals of this kind do point out the relevance of exposure in detemining the potentially affected population under the conditions of the scenario in question (cf. BBK 2016, 47–49).

[11] The range of services to be considered as part of *Daseinsvorsorge* is contested, cf. Knorr (2005) and Ronellenfitsch (2003). On the relation between *Daseinsvorsorge* and CIP cf. Folkers (2017).

[12] For a critical account of the actual universality of electricity supply in Germany see Becker et al. (2014).

the infrastructures[13] and the vulnerability of their customers. Additionally, two different risk management logics are being applied: while seeking to avoid outages foregrounds prevention, developing a capacity to handle service disruptions favours preparedness. In theory, these logics would be perfectly complementary, but actually they might often be undermining each other.

Excursus: two different kinds of domino effects

To illustrate how focussing on exposure due to proximity or vulnerability due to dependency changes the picture it is worth taking a closer look at how *domino effects* are understood in the context of HI and the way they came to be understood in CIP. In the 12. BImSchV the domino effect is dealt with in sect. 15: the operators must be notified by the authorities responsible regarding the probability or severity of HI within facilities or groups of facilities being increased due to their location, the distance between them or the hazardous materials present at the site(s). Apparently, it is spatial proximity and the disposition between facilities containing certain hazardous materials which raise the risk of a HI (make it possible, more likely and/or more severe): the sites are seen to be mutually exposed to the adverse effects an incident in their vicinity might cause. Thus, increasing risk is an effect of the concentration in an area of distinct sources of risk which by way of interacting add to the risk each single facility would bring about. Risk, in this understanding, is related to spatially distinct sources, it can be aggravated by their spatial accumulation and density and can be managed by practices such as "avoidance distances, regulations preventing buildings from being built near to other buildings, and the creation of free spaces to allow for clearance" (November 2004, 277)[14].

Turning to the CI perspective, the *Baseline Protection Concept* states that a facility "may also be affected by events outside of the actual facility, in neighbouring operational areas or traffic facilities to which a special threat potential applies (domino effect). Possible impacts in this respect include the spread of fire from neighbouring facilities, flying debris after an explosion in neighbouring facilities, the failure of supplies after catastrophic events outside of the facility, etc." (BMI 2005b, 14; cf. section 3). This explication of domino effects clearly bears resemblance to the understanding of the term in the 12. BImSchV, but 'failure of supplies' extends it to include a kind of dependency. In the guidelines for *Risk and Crisis Management* domino effects are mentioned in an example dealing with the potential impacts of pandemics. It states that "the availability of many resources and services could be limited or cut off entirely. Due to mutual dependencies, this can lead to a domino effect shutting down much of the government, economy and society" (BMI 2008, 10). The explanation is embedded in an example so its transferability to other contexts might be restricted; nevertheless, it is in the context of dependencies that this particular domino effect is seen to occur. The *CIP Strategy* sees the "disruptions and failures" that "may entail so-called domino and cascade effects" being caused by "the important interdependencies among the various infrastructures" (BMI 2009, 9).

It is worth mentioning that explanations for dependencies in the context of CI regularly include a category of spatially defined interrelations between the facilities usually referred to as "geographic interdependency" according to an extensively quoted publication by Rinaldi et al. (2001, 15): "A geographic interdependency occurs when elements of multiple infrastructures are in close spatial proximity. Given this proximity, events such as an explosion or fire could create correlated disturbances or changes in these geographically interdependent infrastructures" (cf. Riegel 2015a, 1618; Lenz 2009, 25). Furthermore, the practice of the parallel routing of various infrastructures is being problematized (Bundestags-Drucksache 16/10292; Riegel 2015a, 2015b). Yet, it is the interference of functionally dependent sites which appears as the CI-specific aspect of what is referred to as a domino effect.

The way exposure based on spatial proximity is foregrounded in risks associated with HI while vulnerability due to dependency plays a dominant role in the CI perspective reflects two different types of what November (2004, 283) refers to as relations "between risk and territory": "Whereas a contiguous relation is based on distance and the connection between the various elements (by employing a frame of reference such as proximity or closeness), a rela-

[13] On the vulnerability of CI cf. Lenz (2009) and Krings (2011).

[14] As to the role of spatial distances in the context of domino effects cf. (e.g.) LANUV (n.d.); as to managing risks related to hazardous incidents by way of stipulating spatial distances in land-use planning (*Bauleitplanung*) cf. BImSchG (art. 50) and KAS (2010); on spatial distances in the context of protection from emissions in land-use planning cf. (e.g.) MULNV (2007).

tion of connexity highlights the strong link between the various elements, beyond the physical distance that separates them" (ibid.). The dominance of vulnerability – of society *and* infrastructure systems – is seen to be linked to a specific way of conceptualizing security. Aradau (2010, 500–501) describes the notion that societies are "'grounded' in infrastructure" as inherent to CIP: "their functioning, continuity and survival are made possible by the protection of infrastructure". For the US context Collier and Lakoff (2008, 18) make the observation that "[...] what emerged was a way of understanding security threats as problems of system vulnerability. The task of protecting national security came to include ensuring the ongoing functioning of a number of vulnerable systems that were seen as vital to collective life". Kaufmann (2010) draws a connection between CIP and the rise of the notion of *zivile Sicherheit* in Germany: Hereby threats are predominantly considered to be an effect of the constitution of highly modern, interdependent societies and a new type of vulnerability, the vulnerability of 'vital systems', is identified as the basic underlying security issue (ibid., 119; cf. also Kaufmann 2017). In this line of argumentation, the concern for CI is characteristic of conceptualizing security predominantly through vulnerability and addressing security issues by addressing vulnerability.

4.3 Public relations: diverse information policies on site

The 12. BImSchV draws a distinction between two classes of facilities according to type and amount of substances present at the sites as listed in annex I (cf. BImSchV, sect. 2, para. 1-2). While the obligations to inform the public specified in sect. 8a of the ordinance apply to operators of sites in both classes, the additional obligations specified in sect. 11 only apply to operators of sites in the second class. Operators of sites in both classes generally have to make information on the hazardousness of their plant publicly available according to sect. 8a; operators of sites in the second class additionally have to actively provide it to all persons and all facilities frequented by customers potentially affected by an incident at their site according to sect. 11. As specified in annex V of the ordinance, conforming to sect. 8a involves (i.a.) a declaration that the plant is subject to the ordinance, information on the location, information on the operations carried out in the plant, on the hazardous materials present at the site and on appropriate behaviour in case of an incident (cf. BMU 2004, 67–75). To conform to sect. 11 of the 12. BImSchV additional information has to be provided (i.a.) on potential impacts an incident at the site concerned might have on human health and the environment and on measures taken to either prevent or contain them. Providing brochures such as those referred to in the introduction is done in accordance with these passages of the 12. BImSchV.

In the CI context there are also informative brochures, explicitly addressing the public, on the impacts of outages and on appropriate behaviour in such an event (cf. BBK 2015). It is not the nature of the information as such but the level of discreteness that makes a difference: while information on hazardousness is available at the level of distinct facilities, public information on criticality remains on a generic level. Passages of the EU directive on the identification and designation of European critical infrastructures (Council Directive 2008/114/EC) and the German *IT-Security Act* (IT-SiG) reveal that this practice not only relates to the problem of identification: a fundamentally different information policy applies in the context of CI. The relevant passage in the directive reads: "Information concerning the designation of an infrastructure as an ECI [European critical infrastructure] shall be classified at an appropriate level" (Council Directive 2008/114/EC, art. 4; cf. also Commission of the European Communities 2006, 3). The same applies for the criteria to be used for identification purposes (Council Directive 2008/114/EC, art. 3). Accordingly, the legal implementation of the directive in the German *Energy Industry Act* reflects this policy of confidentiality (EnWG, sect. 12g, para. 4). Further, the *IT-Security Act* includes the statement that access shall not be granted to the records of information provided by the operators of the infrastructure elements regarded as critical according to the act (IT-SiG, art. 1, sect. 8d, para. 2; the ordinance itself, however, is not classified, cf. BSI-KritisV).

The reason for the restrictive information policy on CI elements in Council Directive 2008/114/EC is elucidated in the preamble: the importance of observing "the rules of confidentiality" is emphasized "with regard to specific facts about critical infrastructure assets, which could be used to plan and act with a view to causing unacceptable consequences for critical infrastructure installations". The need to withhold information on the criticality of facilities is justified by the possibility that this information could be used to purposely bring about what is actually aimed at being avoided, namely disruption of

service potentially accompanied by the destruction of the infrastructures in question[15]. This practice relates to the "types of threats" to be addressed in the *European Programme for Critical Infrastructure Protection* (Commission of the European Communities 2006, 3): although it declares that "the protection of critical infrastructure will be based on an all hazards approach", the programme recognizes "the threat from terrorism as a priority" (ibid.). Likewise, the German *CIP Strategy* explicitly follows an "all hazards approach" (BMI 2009, 9), while the "terrorist threat" (alongside "natural hazards") is being foregrounded (ibid., 10). In summary, terrorist attacks are not the only threats that both *European Programme for Critical Infrastructure Protection* and the German *CIP Strategy* are taking into account, but they play a prominent role.

As regards the range of threats considered in the context of HI, in its list of operators' general obligations the 12. BImSchV (sect. 3, para. 2) cites operational hazards, environmental hazards and unauthorized interference as those that must be taken into account in arrangements to avoid incidents. Although this rather generic list covers quite a broad range of potential threats, there is evidence that industrial accidents have been most influential in the development of the policy. Pettelkau (1981) lists cases which particularly attracted attention in Germany and ascribes to the *Seveso* accident (Italy, 1976) a "signalling effect" (ibid., 22; my translation; see also Böschen 2003)[16]. At the European level the accident occasioned the adoption of the directive "on major-accident hazards of certain industrial activities" (European Commission 2017; cf. Council Directive 82/501/EEC), which even bears the by-name *Seveso-Directive*. Industrial accidents continued to play a dominant role in developments in this policy area. In 1996, for instance, the directive was amended explicitly "in view of the lessons learned from later accidents" (European Commission 2017; cf. Council Directive 96/82/EC). Just as in CIP, a broader range of threats is generally considered to be relevant in the context of HI, but a certain type of threat – here: industrial accidents – is of outstanding importance. The different focus might have contributed to a permissive or even proactive information policy in the management of risks related to HI.

This, however, needs to be qualified: the 12. BImSchV contains reservations regarding the generally open information policy it promotes. Both in sects. 8a and 11 of the ordinance, a passage is included stating that in order to protect "public or private interest" (my translation) the obligations to inform the public can be suspended. According to sect. 11 (para. 6) some passages of the – otherwise fully available – security report of the site can be withheld from the public in accordance with Council Directive 2003/4/EG "on public access to environmental information". Pursuant to the above-named directive a request for information can be refused i.a. if its disclosure "would adversely affect […] international relations, public security or national defence" (Council Directive 2003/4/EG, art 4, para. 2b). These statements bear resemblance to the argumentation in the context of CIP summarized above; however, they constitute the entitlement to make *exceptions* rather than specifying general restrictions to public information on the hazardousness of specific sites (cf. Jochum 2005, 1360).

The two perspectives exhibit divergent underlying attitudes to informing the public. The European Commission (2015) explains "your right to know" – an expression relating to debates on government transparency – regarding HI related information as follows: "Many environmental laws oblige governments to share information they gather about the state of the environment. This empowers citizens like you, so you can track where potentially hazardous sites are […]. You are entitled to this information […] and you don't have to say why you want it." Its counterpart 'need to know', on the contrary, characterizes restrictive information policies. The *European Programme for Critical Infrastructure Protection*, which counts 'confidentiality' among its principles, uses the expression as follows: "both at EU level and MS [Member State] level, Critical Infrastructure Protection Information (CIPI) will be classified appropriately and access granted only on a need-to-know basis" (Commission of the European Communities 2006, 3). In short, one has to prove a legitimate interest to be given access to otherwise inaccessible information.

Yet, as exemplified in the following, irrespective of the contrariness of the information policies outlined above, conflicts of interest between transparency and confidentiality have surfaced in both

[15] Kaufmann (2010, 115) and Lorenz and Voss (2013, 68) apply the metaphor of 'autoimmunity' in related contexts.

[16] For an extensive account of industrial accidents/accidents involving hazardous materials in the 1970s and 1980s cf. Bockholts and Koehorst (1992). The database ZEMA (*Zentrale Melde- und Auswertestelle für Störfälle und Störungen in verfahrenstechnischen Anlagen*) has been providing information on incidents notifiable according to the 12. BImSchV since the 1990s (UBA, n.d.).

perspectives. After the terrorist attacks of 9/11 a commission (*Störfall-Kommission,* SFK) appointed by the *Ministry for the Environment, Nature Conservation and Nuclear Safety* assessed the need to take action on security regulations for facilities subject to the 12. BImSchV (SFK 2002). Its tasks included giving "recommendations for balancing the legitimate public interest to have access to information on the security of industrial sites" and the risks this might give rise to (ibid., 5; my translation; cf. Jochum 2005). In the CI context, the adoption of Directive 2007/2/EC on "establishing an Infrastructure for Spatial Information in the European Community", the so-called 'INSPIRE-Directive', and its implementation in the German *Geodatenzugangsgesetz* (GeoZG) may serve as an example: As this legislation concerns spatial data on facilities from CI sectors recommendations have been provided to operators on how to conform while protecting the interests of CIP (Geschäftsstelle der Kommission für Geoinformationswirtschaft 2016).

5 Synopsis

While the hazards the perspectives are concerned with can all be characterized as disruptive inasmuch as they do not arise from normal procedures but from exceptional incidents, their impacts – emissions of hazardous substances or outages of common services – are fundamentally different. The governance approach dominant in the management of risks related to HI has been regulative from the beginning and the policy area is organized around a central legislative instrument (12. BImSchV). In the context of CIP, a variety of different instruments has been applied. The 'cooperative approach' emphasizes 'soft' instruments and legislation is declared a means of last resort (BMI 2009, 15). The comparative exploration has brought to light a number of features of the HI and CI perspectives summarized in table 2.

The two perspectives have been shown to work on different levels of **discreteness** (cf. section 4.1): while the focus has always been on clearly identifiable facilities in the HI perspective, identifying facilities as CI components has only recently become feasible. Yet, assessing criticality is nonetheless regarded as a highly context-dependent undertaking. The potential sources of HI have been identified and located at all administrative levels with reference to the 12. BImSchV. By contrast, identification of CI facilities by the BSI-KritisV is restricted to the federal level (and to the sectors within its scope). As a result of employing these different approaches, the sources of risks related to HI have been construed as **site-specific** and **'situated'**, whereas their equivalents in the CI perspective remain comparatively **indistinct** and **'un-situated'**. Putting it in the language of riskscapes: in the HI perspective, the sources of risk are clearly visible from different viewpoints, whereas in the CI perspective consideration of individual facilities might be 'blurred' or they might even be invisible from some points of view.

Starting from the spatiality of the two different risks, the differences in what might be termed their 'internal structure' (re)produced by the practices that adhere to the two perspectives have been identified (cf. section 4.2): the dominant role that **exposure** due to proximity plays in risk management concerning hazardous facilities and the practices foregrounding **vulnerability** due to dependency in the CI perspective. These findings match the observation that a relation of **connexity** between CI components as well as between the infrastructures and their customers is fundamental to the CI perspective, while a relation of **contiguity** between 'hazardous facilities' and those potentially affected by an incident is characteristic of the HI perspective. Putting it differently, another measure of 'distance' (and another conception of 'space') applies to the relations between the 'source of risk' and who or what is 'at risk' in the riskscapes emerging in the two perspectives: while physical distance is paramount in the HI perspective, functional distance counts in the CI perspective. Accordingly, using the same topographic base map, the risks in the HI perspective can be characterized as **focused** and **concentrated** in the area surrounding its source, whereas the risks in the CI perspective appear to be spatially **diffuse** and **dispersed**.

Finally, differentiating between 'perspective' and 'viewpoint' has proved helpful in analyzing the asymmetry in levels of **site-specific information** in the two perspectives (cf. section 4.3): whereas the hazardousness of a site is designated to be public information, its criticality is to remain classified. It is part of official risk-management policy to have the public gear their risk management practices towards 'hazardous facilities' so measures are taken which make the facilities 'visible' from their viewpoint by way of a generally **proactive** information policy. As for CI, site-specific information is deliberately withheld from the public. Following a twofold approach, general awareness of the risks associated with a blackout (or other kinds of CI outages) is desired

Tab. 2: Characteristic features of hazardous incident and critical infrastructure perspectives explored in this paper.

	Hazardous incident perspective	Critical infrastructure perspective
Level of discreteness (identification of sites)	**site-specific, situated** attribution of hazardousness to clearly identifiable sites on the basis of universally applicable thresholds	**indistinct, un-situated** degree of criticality of sites considered context-dependent; no universally applicable thresholds
Dominant risk determinant	**exposure** to hazardous substances	**vulnerability** due to dependency on services
Dominant type of relation	**contiguity** spatial proximity / disposition is decisive	**connexity** functional ties are decisive
Spatial distribution of risk	**focussed, concentrated** risk 'occupies' areas surrounding its source	**diffuse, dispersed** no general restriction of risk to a spatially definable area
Information policy on specific sites	**proactive** legal obligation to share information on hazardousness of sites	**restrictive** information on criticality of specific sites to be treated confidentially

(e.g. BBK 2015), while the circle of addressees destined to share information on the criticality of facilities is **restricted**. In other words, the perspective is to be adopted by the public, but the facilities in question are not to be part of the picture from their viewpoint. The information policies have implications as to who might recognize a facility as a source of what risk, who might treat it as such and, subsequently, whose riskscape it might be included in.

6 Overlaps and outlooks

The two different risks are likely to occupy the same territory "not just metaphorically" and the riskscapes their management (re)produces are likely to "overlap in time and space" (Müller-Mahn and Everts 2013, 24). Given the severe consequences associated with both kinds of threats, what abstract academic language refers to as an 'overlap' might under the most adverse conditions lead to a situation which civil protection terminology refers to as a 'disaster' (UNISDR 2009, 9)[17]: A facility might be hazardous *and* critical, HI might cause damage to CI, and, conversely, CI outages might threaten 'hazardous facilities', and furthermore the practices applied in accordance with each perspective might be conflicting. Thus, the paper will conclude with reflections on the implications the approaches to CI and HI related risks might have on the handling of different kinds of overlap situations. The German civil protection system is subsidiarily organized (cf. Geier 2017) which entails leaving the rather abstract viewpoint of the federal level considered so far to turn to the other administrative levels (i.e. states and municipalities): The management of both CI and HI related risks as well as their potential interactions primarily involve the municipal civil protection authorities on the administrative side and the fire brigades and relief organisations on the operative side. To be clear, rather than making statements on the management of actual situations (which would be a separate paper based on different methods and empirical material), the following reflects upon the conditions for managing overlaps determined by the features of the perspectives explored above. For illustrative purposes, a number of meta-practices, i.e. 'risk management manuals', addressing the work of those involved in civil protection at the local level are selectively referred to. Interestingly, these sources often give the argumentation a new twist: the approaches they present at times do *not* seem to be one-to-one translations of the ideas presented so far for application at the local level. This observation leads to another purpose of this section: Abandoning the restriction necessary so far of considering only one viewpoint, i.e. the viewpoint of the state at federal level in sections 1-5, it seeks to (re)introduce the notion of the management of the two risks as both multi-level and multi-stakeholder issues. Doing so the section will (almost inevitably) raise a number of related research questions, which makes it at least as much an outlook as a conclusion.

[17] In Germany *Katastrophe* is a commonly used term (cf. BHKG). On the appropriate terminology and the problems of its translation cf. Krings and Glade (2017) and on the German civil protection system cf. Geier (2017).

First of all, the separation of the two perspectives outlined section 3 might have an influence on the degree to which CI and HI related risks are seen not in isolation but in conjunction in the first place. At a conceptual level, the formation of an increasingly CI specific understanding of risk has certainly led to a more clear-cut problem definition but it might also have erased links to the HI perspective. Hence, for future research, it might be interesting to investigate the integration of the perspectives in applied contexts, such as the operational planning to be carried out by civil protection institutions. Some of the CIP-related sources consulted make explicit reference to 'hazardous facilities' (cf. Stolzenburg and Müller 2014; HMdIS n.d. a) but more comprehensive analyses of operation plans (or actual operations) would be needed to gain insights into their implementation.

One of these operation plans is the 'action plan critical infrastructure' set up by the fire brigade of the City of Hannover (Lange et al. 2015, 7–8). Remarkably, it refers to a version of the CI sector classification still containing the sector 'hazardous materials', although at federal level it had been superseded several years before (cf. section 3). As to the classification, Lange et al. (2015) quote guidelines on crisis management in blackout situations the work on which had been initiated after a crisis management exercise in the year 2004 (Hiete et al. 2010; BBK n.d.). This observation entails that changes of basic concepts – here: the progressive differentiation between hazardousness and criticality – might not necessarily be observed instantaneously and comprehensively by all stakeholders involved: A certain degree of heterogeneity of the concepts circulating in the web of entwined 'risk management manuals' might be the result. Exploring the transfer of concepts within this web, its potential selectiveness and the reinterpretations happening along the way would be promising subjects for future research on CIP as a 'multi-level governance issue' (cf. Riegel 2015a, 37–46).

The levels of discreteness (cf. section 4.1) and assumptions of the spatial distribution of risk (cf. section 4.2) in the HI and CI perspectives might have an impact on the conditions for anticipating situations in which the two types of threat interfere with each other. As the occurrence of outages is not generally bound to specific areas, it is plausible to assume a comprehensive outage and consider its potential effects on the facilities clearly identified by the 12. BImSchV. This procedure has, for instance, been included in the recommendations of the state of Hessen for operational planning for prolonged and wide-area blackouts (HMdIS n.d. a, 50–52). The conditions for considering the potential effects of HI on CI facilities might be more problematic: The locations of 'hazardous facilities' and the areas 'at risk' in case of a HI are known – but it might not be easy to decide whether or not a CI facility could be affected as long as there is no easy answer to the question 'what is a CI facility?'. Hence, detecting situations in which both risks might 'occupy the same territory' could be technically impeded. Given the multi-level organization of the German civil protection system different understandings as to what facility is to be regarded as critical might cause problems even within the CI perspective: Planning undertaken by different stakeholders might refer to different sets of CI facilities. If, for instance, prioritization of resources at different levels does not consistently take into account the same facilities, conflicts of interest may arise in the case of an incident. Accordingly, whether or not manuals and blueprints for operational planning satisfactorily address the need to compare and, if need be, reconcile approaches of the various stakeholders involved should be looked into.

Operation plans for blackout scenarios, which might serve as an entry point to this subject area, have actually been set up in a number of municipalities during the last few years and a couple of blueprints are available (Regierungspräsidium Karlsruhe 2014; HMdIS n.d. b). Taking a closer look at one example, the above-mentioned plan for the City of Hannover (Lange et al. 2015), reveals that efforts to identify facilities considered as particularly important in blackout situations have been made. The criteria by which objects are selected for inclusion in the accompanying geographic information system – 'in need of protection' or 'systemic for civil protection purposes' (ibid., 9) – offer a first glance at the underlying rationale. Looking into the (different?) approaches to determining relevant sites at local level and exploring their relation to the concept of 'criticality' applied at federal level (cf. section 4.1) could be promising follow-up research activities.

The spatialities incorporated in the practices applied in accordance with the HI and CI perspectives expounded in section 4.2 could have practical relevance in that they might run counter to each other. A relation of contiguity to a focussed source of risk is reflected, for example, in the practice of zoning described in the regulations for fire brigades for operations involving

hazardous materials (*Feuerwehr-Dienstvorschrift 500,* AFKzV 2012). According to these regulations two different zones on the basis of spatial distance to the source are to be installed (ibid., 28; cf. Fig. 1): Only members of relief units wearing protective gear are allowed to enter the 'danger zone' surrounded by a 'restricted zone' only to be entered by authorized personnel. Evacuations and restrictions on entering the zones certainly reduce exposure of people in the immediate surroundings (and facilitate emergency management procedures). Yet their implementation might be problematic when the operation of CI facilities situated in the zones requires the presence of personnel e.g. in the interest of people and objects in a wider area who are dependent on the services provided. The need to continue CI operations might call for deliberate decision making and, potentially, laborious arrangements further adding complexity to the situation. If, in extreme cases, a 'hazardous critical infrastructure' were involved, deciding upon whether or not to shut down the affected facility might even involve weighing up its criticality and its hazardousness against each other.

Whether or not the problems described above (and maybe others) have surfaced in advance, may considerably impact on effectively managing an emergency situation once it has come about. Hence, it is crucial that those who plan and carry out operations are comprehensively informed. The set-up of 'external emergency plans' at municipal level stipulated by the civil protection laws of the states (e.g. BHKG, sect. 30) establishes a direct and stable line of information exchange as concerns facilities subject to the 12. BImSchV. In the documents relating to the CI perspective, the importance of cooperating with civil protection institutions is being underlined (e.g. BMI 2009; BBK 2012), but there is no equally well-defined channel for exchanging information. An empirical study conducted in German cities reveals that basic information on changes to infrastructure systems and contact persons on the operators' side might not be regularly communicated to the local civil protection authorities (Schmidt and Matern 2015, 78–79). This observation raises the issue of ensuring information exchange between various stakeholders operating at different levels who, moreover, might all regard part of this information as internal or even confidential. An approach to attending to the issue in a legal framework can be found in the civil protection law of the state of North Rhine-Westphalia (*Gesetz über den Brandschutz, die Hilfeleistung und den Katastrophenschutz,*

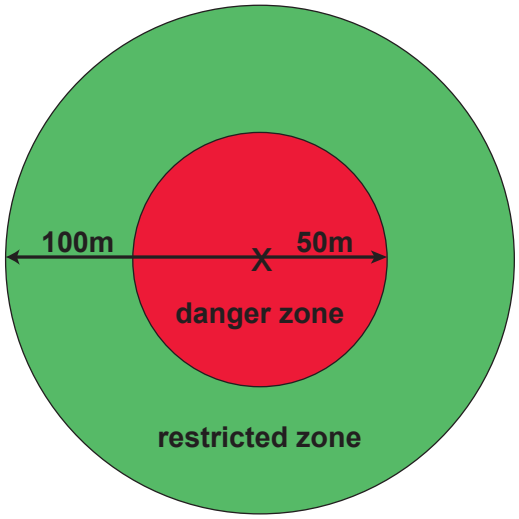

Fig. 1: Schematic depiction of position and minimum size of 'danger zone' and 'restricted zone' relative to the source of danger in the center (draft based on AFKZV 2012, 28; my translation).

BHKG) after its comprehensive amendment in 2015. Operators of local water and energy supply systems are to inform the municipal administration on the location of facilities which play a "significant" role in supplying the population and which are "particularly in need of protection" (BHKG, sect. 47, para. 2, my translation). Additionally, spatial extent and expected duration of outages of supply have to be reported (ibid.). However, the problem of organizing a constant flow of necessary information does not yet seem to have been solved comprehensively in the CIP context.

The approaches to providing site-specific information to the public applied in accordance with the HI and CI perspectives[18] (cf. section 4.3) have surfaced as contradictory not only in theory but also in practice. Kraemer and Stening (2006, 73) characterise the issue of balancing CIP and informing the public as an open question in the course material on risk management with regard to 'hazardous sites' at a training institution for fire-fighters. Accordingly, this seems to be another case of contradictory practices in risk management concerned with potentially one and the same facility. The rules of transparency as regards facilities prone to HI and of confidentiality in CIP being diametrically opposed, it seems unlikely that a coherent approach to informing the public is an option. Yet, systematically

[18] For an example of efforts taken at the local administrative level to inform the public about risks generally associated with outages cf. Landeshauptstadt Dresden (2016).

addressing the issue of conflicting practices might support the practitioners in appropriately handling information. Instead of treating the policy of confidentiality in accordance with the CI perspective as a given circumstance, Lorenz (2010, 77) recommends entering into a risk communication process to broadly discuss the intrinsically problematic relation between the public's right to know about risks they might be affected by and the sensitivity of risk-related information – including the crucial questions: What interest ranks higher? And who is to decide? The question as to whether or not there could be any desirable effects to a more permissive information policy on CI facilities has not yet received much attention.

The material used to illustrate and support the argumentation in section 6 comprises meta-practices which seek to structure the actions taken in concrete situations. Yet, the process of pointing out the conflicts that the internal logics of the two perspectives could cause may in itself contribute to 'setting the scene' for a more 'on the ground' research agenda. For future research, leaving the meta-level of description and turning to case studies might not only reveal the effects of the meta-practices on the last links in the chain of risk management but disclose interactions of the two perspectives their generic depictions do not account for. This might not only, at an academic level, further explore the qualities of riskscapes as a tool (Müller-Mahn and Everts 2013, 24) but extend the knowledge base for integrated approaches to managing risks related to facilities be they hazardous, or critical, or even both.

Acknowledgements

I would like to thank Florian Neisser for his comments on the manuscript and his support at various stages of the work in progress, the two anonymous reviewers for providing me with constructive remarks and valuable food for thought, and the patient and thoughtful proof reader without whom this paper would not look the same.

References

12. BImSchV (Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes – Störfall-Verordnung) in der Fassung der Bekanntmachung vom 15. März 2017 (BGBl. I S. 483), zuletzt geändert durch Artikel 58 des Gesetzes vom 29. März 2017 (BGBl. I S. 626).

Aden, H. (2012): Umweltpolitik. Wiesbaden.

AFKzV (Ausschuss für Feuerwehrangelegenheiten, Katastrophenschutz und zivile Verteidigung des Arbeitskreises V der Ständigen Konferenz der Innenministerkonferenz und -senatoren der Länder) (2012): Feuerwehr-Dienstvorschrift FwDV 500. Einheiten im ABC-Einsatz. (Stand: Januar 2012). http://www.idf.nrw.de/projekte/pg_fwdv/pdf/fwdv500_jan2012.pdf (Date: 01.09.2017)

Appadurai, A. (1990): Disjuncture and difference in the global cultural economy. In: Theory, Culture & Society 7 (2-3), 295–310. https://doi.org/10.1177/026327690007002017

Aradau, C. (2010): Security that matters: critical infrastructure and objects of protection. In: Security Dialogue 41 (5), 491–514. https://doi.org/10.1177/0967010610382687

BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) (ed.) (2012): Schutzkonzepte Kritischer Infrastrukturen im Bevölkerungsschutz. Ziele, Zielgruppen, Bestandteile und Umsetzung im BBK. Wissenschaftsforum 11. Bonn. http://www.kritis.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Wissenschaftsforum/Bd_11_Schutzkonzepte_KRITIS.pdf (Date: 01.09.2017)

– (ed.) (2015): Stromausfall. Vorsorge und Selbsthilfe. Bonn. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Stromausfall_Vorsorge_u_Selbsthilfe.pdf (Date: 01.09.2017)

– (ed.) (2016): Sicherheit der Trinkwasserversorgung. Teil 1: Risikoanalyse. Praxis im Bevölkerungsschutz 15. Bonn. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band-15_Praxis_BS_Trinkwasserversorgung.pdf (Date: 01.09.2017)

– (2017): Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten. Arbeitshilfe für die Anwendung im Bevölkerungsschutz. Praxis im Bevölkerungsschutz 20. Bonn. https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band_20_Praxis_BS_Schutz_Kritis_Identifizierung.pdf (Date: 29.12.2017)

– (n.d.): Der Stromausfall und seine Auswirkungen. http://www.bbk.bund.de/DE/TopThema/TT_2010/Stromausfall-und-Auswirkungen.html (Date: 01.09.2017)

BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) and BSI (Bundesamt für Sicherheit in der Informationstechnik) (2011): Critical Infrastructure Sectors and Subsectors. (published online: 13.05.2011) http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/sectors/sectors.html (Date: 01.09.2017)

BBSR (Bundesinstitut für Bau-, Stadt- und Raumforschung) (ed.) (2012): Raumordnungsbericht 2011. Bonn. http://www.bbsr.bund.de/BBSR/DE/Veroeffentlichungen/Sonderveroeffentlichungen/2012/DL_ROB2011.pdf (Date: 01.09.2017)

Beck, U. (1986): Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt a.M.

Becker, B.; Kouschil, K. and Naumann, M. (2014): Armut und Infrastruktur: das Beispiel Energiearmut. In: Geographische Rundschau 2014 (10), 10–17.

BHKG (Gesetz über den Brandschutz, die Hilfeleistung und den Katastrophenschutz) vom 17. Dezember 2015 (Fn 1), Artikel 1 des Gesetzes vom 17. Dezember 2015 (GV. NRW. S. 886).

BImSchG (Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge – Bundes-Immissionsschutzgesetz). In der Fassung der Bekanntmachung vom 17. Mai 2013 (BGBl. I S. 1274), zuletzt geändert durch Artikel 3 des Gesetzes vom 29. Mai 2017 (BGBl. I S. 1298).

BMI (Bundesministerium des Innern) (ed.) (2005a): Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI). Berlin. http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf (Date: 01.09.2017)

– (ed.) (2005b): Protection of critical infrastructures – baseline protection concept. Recommendation for companies. Berlin. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Basisschutzkonzept_engl.pdf (Date: 01.09.2017)

– (ed.) (2005c): Schutz Kritischer Infrastrukturen – Basisschutzkonzept. Empfehlungen für Unternehmen. Berlin. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Basisschutzkonzept_Kritis.pdf (Date: 01.09.2017)

– (ed.) (2008): Protecting critical infrastructures – risk and crisis management. A guide for companies and government authorities. Berlin. https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Protecting-Critical-Infrastructures.pdf (Date: 01.09.2017)

– (ed.) (2009): National strategy for critical infrastructure protection (CIP strategy). Berlin. http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf (Date: 01.09.2017)

– (ed.) (2011a): Cyber-Sicherheitsstrategie für Deutschland. Berlin. http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/2016_16_11_Cyber_Sicherheitsstrategie2011.pdf (Date: 01.09.2017)

– (ed) (2011b): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden. Berlin. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Leitfaden_Schutz-Kritis.pdf (Date: 01.09.2017)

– (ed.) (2016): Cyber-Sicherheitsstrategie für Deutschland 2016. Berlin. https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (Date: 01.09.2017)

– (ed.) (n.d.): Umsetzungsplan KRITIS zum Nationalen Plan zum Schutz der Informationsinfrastrukturen. Berlin. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.pdf (Date: 01.09.2017)

BMU (Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit) (ed.) (2004): Vollzugshilfe zur Störfall-Verordnung vom März 2004. Bonn. http://www.bmub.bund.de/fileadmin/Daten_BMU/Download_PDF/Wirtschaft_und_Umwelt/vollzugshilfe_stoerfall_vo.pdf (Date: 01.09.2017)

Bockholts, P. and Koehorst, L. J. B. (1992): Handbuch Störfälle II – Dokumentation über Störfälle in industriellen Anlagen oder mit gefährlichen Stoffen im Zeitraum von 1981 bis 1986. Materialien Umweltbundesamt Forschungsbericht 10409109. Berlin.

Böschen, S. (2003): Katastrophe und institutionelle Lernfähigkeit. Seveso als ambivalenter Wendepunkt der Chemiepolitik. In: Clausen, L.; Geenen, E. M. and Macamo, E. (eds.): Entsetzliche soziale Prozesse. Theorie und Empirie der Katastrophe. Konflikte, Krisen und Katastrophen – in sozialer und kultureller Sicht 1. Münster, 139–162.

Brunner, E. M. and Suter, M. (2008): International CIIP-Handbook 2008/2009. An inventory of 25 national and 7 international critical information infrastructure policies. Zurich.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2004): Annual Report 2003. Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Annualreport/BSI-AnnualReport2003_pdf (Date: 17.01.2018)

BSI-KritisV (BSI-Kritisverordnung) vom 22. April 2016 (BGBl. I S. 958) zuletzt geändert durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. I S. 1903).

Bundestags-Drucksache VI/2710 vom 14.10.1971. Umweltprogramm der Bundesregierung. http://dipbt.bundestag.de/doc/btd/06/027/0602710.pdf (Date: 01.09.2017)

Bundestags-Drucksache 13/7753 vom 22.05.1997. Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Dr. Manuel Kiper und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 13/7594. Lage der IT Sicherheit in Deutschland. http://dipbt.bundestag.de/doc/btd/13/077/1307753.pdf (Date: 01.09.2017)

Bundestags-Drucksache 16/10292 vom 22.09.2008. Entwurf eines Gesetzes zur Neufassung des Raumordnungsgesetzes und zur Änderung anderer Vorschriften (GeROG). http://dip21.bundestag.de/dip21/btd/16/102/1610292.pdf (Date: 01.09.2017)

Claus, F.; Wiedemann, P. M.; Bloser, M.; Matzke, M.; Schütz, H. and Vossebürger, P. (1999): Handlungsempfehlungen zur Information der Öffentlichkeit (nach § 11a Störfall-Verordnung). https://www.umweltbundesamt.de/sites/default/files/medien/publikation/long/257.pdf (Date: 01.09.2017)

Collier, S. J. and Lakoff, A. (2008): The vulnerability of vital systems. How 'critical infrastructure' became a security problem. In: Dunn Cavelty, M. and Søby Kristensen, K. (eds.): Securing the homeland: critical infrastructure, risk and (in)security. London, 17–39.

Commission of the European Communities (2006): Communication from the Commission on a European Programme for Critical Infrastructure Protection. COM (2006) 786 final. Brussels. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=DE (Date: 01.09.2017)

Council Directive 82/501/EEC on the major-accident hazards of certain industrial activities of 24 June 1982 (OJ L 230/1).

Council Directive 96/82/EC on the control of major-accident hazards involving dangerous substances of 9 December 1996 (OJ L 10/13).

Council Directive 2003/4/EC on public access to environmental information and repealing Council Directive 90/313/EEC of 28 January 2003 (OJ L 41/26).

Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection of 8 December 2008 (OJ L 345/75).

Council Directive 2012/18/EU on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC of 4 July 2012 (OJ L 197/1).

Directive 2007/2/EC of the European Parliament and of the Council establishing an infrastructure for spatial information in the European Community (INSPIRE) of 14 March 2007 (OJ L 108/1).

Einig, K. (2008): Regulierung der Daseinsvorsorge als Aufgabe der Raumordnung im Gewährleistungsstaat. In: Informationen zur Raumentwicklung 2008 (1/2), 17–40.

EnBW (Energie Baden-Württemberg AG - Heizkraftwerk Heilbronn) (2016): Sicherheit für unsere Nachbarn. Information der Öffentlichkeit nach § 11 Störfallverordnung. Heilbronn. https://www.enbw.com/media/konzern/docs/ezg/stoerfallbroschuere-heilbronn.pdf (Date: 01.09.2017)

EnSiG (Gesetz zur Sicherung der Energieversorgung – Energiesicherungsgesetz 1975) vom 20. Dezember 1974 (BGBl. I S. 3681), zuletzt geändert durch Artikel 324 der Verordnung vom 31. August 2015 (BGBl. I S. 1474).

EnWG (Gesetz über die Elektrizitäts- und Gasversorgung - Energiewirtschaftsgesetz) vom 7. Juli 2005 (BGBl. I S. 1970, 3621), zuletzt geändert durch Artikel 13 des Gesetzes vom 29. Mai 2017 (BGBl. I S. 1298).

European Commission (2013): Commission staff working document on a new approach to the European programme for critical infrastructure protection. Making European infrastructures more secure. SWD (2013) 318 final. Brussels. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_38_on_epcip_en.pdf (Date 01.09.2017)

– (2015): Your right to know. (last updated: 14.10.2015). http://ec.europa.eu/environment/basics/benefits-law/right2know/index_en.htm (Date: 01.09.2017)

– (2017): The Seveso Directive - Prevention, preparedness and response. (last updated: 24.08.2017). http://ec.europa.eu/environment/seveso/ (Date: 01.09.2017)

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

Folkers, A. (2017): Existential provisions: the technopolitics of public infrastructure. In: Environment and Planning D: Society and Space 35 (5), 855–874. https://doi.org/10.1177/0263775817698699

Geier, W. (2017): Strukturen, Zuständigkeiten, Aufgaben und Akteure. In: Karutz, H.; Geier, W. and Mitschke, T. (eds.): Bevölkerungsschutz. Notfallvorsorge und Krisenmanagement in Theorie und Praxis. Berlin. 93–128.

Geipel, R. (1982): Wahrnehmung und Bewertung sperriger Infrastruktur durch die Regionalbevölkerung. In: Niedenzu, A.; Stöckl, H. and Geipel, R. (eds.): Wahrnehmung und Bewertung sperriger Infrastruktur. Münchener Geographische Hefte 47. Regensburg, 7–15.

GeoZG (Gesetz über den Zugang zu digitalen Geodaten – Geodatenzugangsgesetz) vom 10. Februar 2009 (BGBl. I S. 278) Artikel 1 des Gesetzes vom 7. November 2012.

Geschäftsstelle der Kommission für Geoinformationswirtschaft (bei der Bundesanstalt für Geowissenschaften und Rohstoffe) (2016) (ed.): Bereitstellung von Metadaten zu INSPIRE-relevanten Geodatensätzen durch Ver- und Entsorgungsunternehmen. Handlungsempfehlung. Hannover. http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/HE_Bereitstellung_Metadaten_durch_Ver_Entsorgungsunternehmen.pdf (Date: 01.09.2017)

Hecht, D. (2003): Die räumliche Ausbreitung von Risiken. In: Karl, H. and Pohl, J. (eds.): Raumorientiertes Risikomanagement in Technik und Umwelt. Katastrophenvorsorge durch Raumplanung. Forschungs- und Sitzungsberichte 220. Hannover, 7–34.

Hiete, M.; Merz, M.; Trinks, C.; Grambs, W. and Thiede, T. (2010): Krisenhandbuch Stromausfall. Kurzfassung. Krisenmanagement bei einer großflächigen Unter-

brechung der Stromversorgung am Beispiel Baden-Württemberg. Stuttgart. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Krisenhandbuch_Stromausfall_Kurzfassung_pdf.pdf (Date: 01.09.2017)

HMdIS (Hessisches Ministerium des Innern und für Sport) (n.d. a): Rahmenempfehlungen zur Einsatzplanung des Brand- und Katastrophenschutzes bei flächendeckendem, langandauerndem Stromausfall. Wiesbaden. https://innen.hessen.de/sites/default/files/media/hmdis/handlungsempfehlung_stromausfall_.pdf (Date: 01.09.2017)

– (n.d. b): Mustereinsatzplan Stromausfall für Feuerwehren bei flächendeckendem, langandauerndem Stromausfall. Wiesbaden. https://innen.hessen.de/sites/default/files/media/hmdis/anlage_1_mustereinsatzplan_stromausfall_feuerwehren_.pdf (Date: 01.09.2017)

Huff, T. (2015): Natur und Industrie im Sozialismus. Eine Umweltgeschichte der DDR. Umwelt und Gesellschaft 13. Göttingen.

IT-SiG (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I S.1324).

Jochum, C. (2005): Was hat Anlagensicherheit mit Terrorismus zu tun? In: Chemie Ingenieur Technik 77 (9), 1356–1361. https://doi.org/10.1002/cite.200500090

John-Koch, M. (2014): Schutz Kritischer Infrastrukturen – Quo Vadis? In: Bevölkerungsschutz 2014 (4), 2–5.

– (2017): Kritische Infrastrukturen. In: Karutz, H.; Geier, W. and Mitschke, T. (eds.): Bevölkerungsschutz. Notfallvorsorge und Krisenmanagement in Theorie und Praxis. Heidelberg, 185–193.

Kaufmann, S. (2010): Zivile Sicherheit: Vom Aufstieg eines Topos. In: Hempel, L.; Krasmann, S. and Bröckling, U. (eds.): Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Leviathan Sonderhefte 25. Wiesbaden, 101–123.

– (2017): Das Themenfeld „Zivile Sicherheit. In: Gusy, C.; Kugelmann, D. and Würtenberger, T. (eds.): Rechtshandbuch Zivile Sicherheit. Berlin, 3–22.

KAS (Kommission für Anlagensicherheit beim Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit) (2010): Leitfaden. Empfehlungen für Abstände zwischen Betriebsbereichen nach der Störfall-Verordnung und schutzbedürftigen Gebieten im Rahmen der Bauleitplanung – Umsetzung §50 BImSchG. Arbeitsgruppe „Fortschreibung des Leitfadens SFK/TAA-GS-1". (KAS-18). Bonn. http://www.kas-bmu.de/publikationen/kas/KAS_18.pdf (01.09.2017)

Kloepfer, M. (2010): Einleitung. In: Kloepfer, M. (ed.): Schutz Kritischer Infrastrukturen. IT und Energie. Schriften zum Katastrophenrecht 3. Baden-Baden, 9–19.

– (2015): Handbuch des Katastrophenrechts. Bevölkerungsschutzrecht, Brandschutzrecht, Katastrophenschutzrecht, Katastrophenvermeidungsrecht, Rettungsdienstrecht, Zivilschutzrecht. Schriften zum Katastrophenrecht 9. Baden-Baden.

Knorr, A. (2005): Gemeinwohl und Daseinsvorsorge in der Infrastrukturpolitik. In: Hartwig, K.-H. and Knorr, A. (eds.): Neuere Entwicklungen in der Infrastrukturpolitik. Beiträge aus dem Institut für Verkehrswissenschaft an der Universität Münster 157. Göttingen, 32–53.

Koch, L. (2016): Heart of Darkness. Über das katastrophische Imaginäre des Blackouts. In: Behemoth 9 (1), 58–76. https://doi.org/10.6094/behemoth.2016.9.1.891

Kraemer, T. and Stening, A. (2006): Gefahrenabwehrpläne & Externe Notfallpläne. Seminar für Führungskräfte 16/2006 am Institut der Feuerwehr NRW, 26.09.2006. http://www.idf.nrw.de/service/downloads/pdf/notfallplanung_idfnrw001.pdf (Date: 01.09.2017)

Kraftwerk Wilhelmshaven (2016): Informationen für die Nachbarn des Uniper Kraftwerks Wilhelmshaven und die Öffentlichkeit gemäß § 11 der Störfallverordnung. Wilhelmshaven. https://www.uniper.energy/content/dam/uniper-corporate/documents/de/wilhelmshaven/KW_Wilhelmshaven_Information_Stoerfallverordnung_2016.pdf (Date: 01.09.2017)

Krings, S. (2011): Verwundbarkeit Kritischer Infrastruktur gegenüber Hochwasserereignissen. In: BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) (ed.): Indikatoren zur Abschätzung von Vulnerabilität und Bewältigungspotenzialen am Beispiel von wasserbezogenen Naturgefahren in urbanen Räumen. Forschung im Bevölkerungsschutz 13. Bonn, 35–94. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenForschung/FiB_Band13.pdf (Date: 01.09.2017)

Krings, S. and Glade, T. (2017): Terminologische Normierungen und Diskussionen. In: Karutz, H.; Geier, W. and Mitschke, T. (eds.): Bevölkerungsschutz. Notfallvorsorge und Krisenmanagement in Theorie und Praxis. Heidelberg, 29–54.

Landeshauptstadt Dresden (ed.) (2016): Stromausfall – wie vorsorgen und handeln? Bürgerinformation. Dresden. https://www.dresden.de/media/pdf/feuerwehr/katastrophenschutz/pdfHZStromausfall16.pdf (Date: 01.09.2017)

Lange, C.; Henke, A. and Kariger, M. (2015): Hannover: Einsatzplanung ‚Kritische Infrastrukturen'. Einsatzplan ‚KRITIS' mit Schwerpunkt Stromausfall wurde umgesetzt. In: Brandschutz 2015 (1), 6–10.

LANUV (Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfahlen) (n.d.): Domino-Effekt. https://www.lanuv.nrw.de/umwelt/industrieanlagen/anlagensicherheit/stoerfall-verordnung/dominoeffekt/ (Date: 01.09.2017)

Lauwe, P. (2016): Konzeption Zivile Verteidigung – Auswirkungen auf Kritische Infrastrukturen. In: Crisis Prevention 2016 (4), 17–19.

Lauwe, P. and Riegel, C. (2008): Schutz Kritischer Infrastrukturen – Konzepte zur Versorgungssicherheit. In: Informationen zur Raumentwicklung 2008 (1/2), 113–125.

Lenz, S. (2009): Vulnerabilität Kritischer Infrastrukturen. Forschung im Bevölkerungsschutz 4. Bonn. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenForschung/FiB_Band4.pdf (Date: 01.09.2017)

Lorenz, D. F. (2010): Kritische Infrastrukturen aus Sicht der Bevölkerung. Schriftenreihe Sicherheit 3. Berlin. http://www.sicherheit-forschung.de/publikationen/schriftenreihe_neu/sr_v_v/sr_3.pdf (Date 01.09.2017)

Lorenz, D. F. and Voss, M. (2013): „Not a political problem". Die Bevölkerung im Diskurs um Kritische Infrastrukturen. In: Hempel, L.; Bartels, M. and Markwart, T. (eds.): Aufbruch ins Unversicherbare. Zum Katastrophendiskurs der Gegenwart. Bielefeld, 53–94.

Müller-Mahn, D. and Everts, J. (2013): Riskscapes. The spatial dimensions of risk. In: Müller-Mahn, D. (ed.): The spatial dimension of tisk. How geography shapes the emergence of riskscapes. London, 22–36.

MULNV (Ministerium für Umwelt und Naturschutz, Landwirtschaft und Verbraucherschutz) (2007): Runderlass des Ministeriums für Umwelt und Naturschutz, Landwirtschaft und Verbraucherschutz - V-3 - 8804.25.1 vom 6.6.2007. Abstände zwischen Industrie- bzw. Gewerbegebieten und Wohngebieten im Rahmen der Bauleitplanung und sonstige für den Immissionsschutz bedeutsame Abstände (Abstandserlass). https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=10000000000000000301 (Date: 01.09.2017)

November, V. (2004): Being close to risk. From proximity to connexity. In: International Journal of Sustainable Development: Values, Knowledge, Environment, Economy, Production, Technology (3) 7, 273–286. https://doi.org/10.1504/IJSD.2004.005958

Petermann, T.; Bradke, H.; Lüllmann, A.; Poetzsch, M. and Riehm, U. (2011): What happens during a blackout? Consequences of a prolonged and wide-ranging power outage. Technology Assessment Studies Series 4. Norderstedt. http://www.tab-beim-bundestag.de/en/pdf/publications/books/petermann-etal-2011-141.pdf (Date: 01.09.2017)

Pettelkau, H.-J. (1981): Gefahrenabwehr durch die Störfall-Verordnung. In: Zivilverteidigung, 1981 (1), 19–26.

PCCIP (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. https://fas.org/sgp/library/pccip.pdf (Date: 01.09.2017)

Radkau, J. (2011): Die Ära der Ökologie. Eine Weltgeschichte. München.

Regierungspräsidium Karlsruhe (2014): Musternotfallplan Stromausfall. Handlungsempfehlungen zur Vorbereitung auf einen flächendeckenden und langanhaltenden Stromausfall. Karlsruhe. https://rp.baden-wuerttemberg.de/Themen/Sicherheit/Documents/MusternotfallplanStromausfall.pdf (Date: 01.09.2017)

Riegel, C. (2015a): Die Berücksichtigung des Schutzes Kritischer Infrastrukturen in der Raumplanung. Zum Stellenwert des KRITIS-Grundsatzes im Raumordnungsgesetz. Schriftenreihe des Instituts für Stadtbauwesen und Stadtverkehr 59. Aachen. http://publications.rwth-aachen.de/record/479433/files/479433.pdf (Date: 01.09.2017)

– (2015b): Spatial criticality – identifying CIP hot-spots for German regional planning. In: International Journal of Critical Infrastructures 11 (3), 265–277. https://doi.org/10.1504/IJCIS.2015.072157

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

ROG (Raumordnungsgesetz) vom 22. Dezember 2008 (BGBl. I S. 2986), zuletzt geändert durch Artikel 5 Satz 2 des Gesetzes vom 23. Mai 2017 (BGBl. I S. 1245).

Ronellenfitsch, M. (2003): Daseinsvorsorge als Rechtsbegriff. Aktuelle Entwicklungen im nationalen und europäischen Recht. In: Blümel, W. (ed.): Ernst Forsthoff. Kolloquium aus Anlaß des 100. Geburtstags von Prof. Dr. Dr. h.c. Ernst Forsthoff. Berlin, 53–114.

Schmidt, M. and Matern, A. (2015): Sektorübergreifende Koordination als Herausforderung nachhaltiger Infrastrukturentwicklung in Städten. In: Informationen zur modernen Stadtgeschichte 2015 (1), 70–81.

Schulze, T. (2006): Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA. Wiesbaden.

Star, S. L. (1999): The ethnography of infrastructure. In: American Behavioral Scientist 43 (3), 377–391.

Stolzenburg, K. and Müller, J. (2014): Zur Identifizierung Kritischer Infrastrukturen. Methodisches Vorgehen und ein Praxisbeispiel aus Waldeck-Frankenberg. In: Bevölkerungsschutz 2015 (1), 6–11.

SFK (Störfall-Kommission beim Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit) (1999): Abschlußbericht. Schadensbegrenzung bei Dennoch-Störfällen. Empfehlungen für Kriterien zur Abgrenzung von Dennoch-Störfällen und für Vorkehrungen zur Begrenzung ihrer Auswirkungen. (SFK-GS-26). http://www.kas-bmu.de/publikationen/sfk/sfk_gs_26.pdf (Date: 01.09.2017)

– (2002): Leitfaden Maßnahmen gegen Eingriffe Unbefugter der ad hoc- Arbeitsgruppe „Eingriffe Unbefugter".

(SFK-GS-38). http://www.kas-bmu.de/publikationen/sfk/sfk_gs_38.pdf (Date: 01.09.2017)

UBA (Umweltbundesamt) (ed.) (2015): 1974-2014. 40 Jahre Umweltbundesamt. Dessau-Roßlau. https://www.umweltbundesamt.de/sites/default/files/medien/376/publikationen/40_jahre_umweltbundesamt.pdf (Date: 01.09.2017)

– (n.d.): Zentrale Melde- und Auswertestelle für Störfälle und Störungen in verfahrenstechnischen Anlagen (ZEMA). Dessau-Roßlau. http://www.infosis.uba.de/index.php/de/zema/index.html (Date: 01.09.2017)

UNISDR (United Nations International Strategy for Disaster Reduction) (2009): UNISDR Terminology on Disaster Risk Reduction. Geneva. http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf (Date: 01.09.2017)

Vossschmidt, S. (2016): Rechtsgrundlagen des Bevölkerungsschutzrechtes unter besonderer Berücksichtigung der Bundeskompetenzen im Bevölkerungsschutz. In: Kuhlmey, M. and Freudenberg, D. (eds.): Krisenmanagement – Bevölkerungsschutz. Lehrstoffsammlung. Berlin, 389–464.

Weyl, H. (1978): Planerische und institutionelle Aspekte bei der Konzipierung kerntechnischer Anlagen. Hannover.

Wiater, P. (2013): Sicherheitspolitik zwischen Staat und Markt. Der Schutz Kritischer Infrastrukturen. Freiburger Studien des Centre for Security and Society 6. Baden-Baden.

Wiater, P. (2017): Bürger und Unternehmen als Akteure der Zivilen Sicherheit. In: Gusy, C.; Kugelmann, D. and Würtenberger, T. (eds.): Rechtshandbuch Zivile Sicherheit. Berlin, 225–245.

ZSKG (Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes – Zivilschutz- und Katastrophenhilfegesetz) vom 25.03.1997 (BGBl. I S. 726), zuletzt geändert durch Artikel 2 Nr. 1 des Gesetzes vom 29.07.2009 (BGBl. I S. 2350).

Author

Susanne Krings
Department of Geography
University of Bonn
Meckenheimer Allee 166
53115 Bonn
Germany
susanne.krings@uni-bonn.de