Common Criteria for the Assessment of Critical Infrastructures

Article *in* International Journal of Disaster Risk Science · March 2011

DOI: 10.1007/s13753-011-0002-y

CITATIONS
67

READS
983

1 author:

Alexander Fekete
TH Köln - University of Applied Sciences
140 PUBLICATIONS **1,133** CITATIONS

SEE PROFILE

Int. J. Disaster Risk Sci. 2011, 2 (1): 15–24
doi:10.1007/s13753-011-0002-y

ARTICLE

Common Criteria for the Assessment of Critical Infrastructures

Alexander Fekete*

Federal Office of Civil Protection and Disaster Assistance, 53008 Bonn, Germany

Abstract Society is reliant on infrastructure services, such as information and communication technology, energy, water, and food supply, but also on governmental, cultural, and search and rescue organizations. The goal of project Kritis-KAT at the Federal Office of Civil Protection and Disaster Assistance in Germany is the development of generic criteria for the identification and evaluation of infrastructures regarded as "critical" for society. Acknowledging that full protection against all threats and cascading effects is not possible, the approach focuses on the impacts rather than the prevention of threats. The development of generic criteria requires the prioritization of infrastructures and identification of their key characteristics for civil protection purposes, risk management activities, and strategic proactive planning. For this purpose, the development of a national critical infrastructure priority inventory is based on a thorough examination of the range of criteria typically used in similar approaches. The specific focus of this paper is to identify and simplify essential characteristics of infrastructure criticality. The main outcome of this study is the development of common criteria generally applicable to a variety of infrastructures.

Keywords civil protection, criteria, critical infrastructure, criticality, national inventory

1 Introduction

Infrastructures are primarily conceived as technical structures, built by humans to facilitate the distribution of goods and services. For centuries, such infrastructures have existed and society has made itself dependent on such support. Progress and civilization are major drivers behind an ever increasing self-induced dependency on the mass-distribution of information, goods, and services. The availability of infrastructures provides high living standards in urban as well as in rural environments. Livelihoods are at the same time dependent on them and service interruptions are mainly perceived to be negative. Influencing factors for an increasing dependency on infrastructure services are ongoing urbanization, economic globalization, and developments in information technology, for instance. These developments bring prosperity, but also expose society to new risks. One remarkable feature of infrastructures is that despite most of them being technical structures, they are almost invisible to the end user, the customer at home. There is an almost blind trust in the daily availability of essential services, which aggravates the element of surprise in a blackout. The criticality of infrastructure services becomes most evident and visible in case of a failure, when services and resources are suddenly not available anymore.

1.1 Demand for Simplified Concepts

There is a need for simple, feasible, and standardized criticality analyses (Theoharidou, Kotzanikolaou, and Gritzalis 2009) despite the wealth of knowledge already created. The development of criticality criteria, or infrastructure-related risk criteria, is an ongoing activity in many countries, for example Canada (Robert et al. 2003), the Netherlands (Vrijling et al. 2004), Switzerland (Swiss Federal Office for Civil Protection 2009), the United Kingdom (UKCO 2010), the United States (Moteff 2007), or even in some provinces, for example, British Columbia (PEP 2007), as well as within the EU for all European countries (EC 2008). Many more countries have published a strategy that typically is the preliminary step to the identification process, for example Australia (Australian Government 2010) and Germany (Federal Ministry of the Interior of Germany 2009). Criticality analyses make use of different methods for the identification of criticality. Expert and operator interviews provide a quick overview and crucial information. Calculations and modeling methods help to understand systems and improve prediction of failures. In principle, criticality can be identified by looking at the infrastructure elements or nodes, the flow of goods and commodities, customer needs, capabilities of search and rescue organizations, and resources for mitigation.

1.2 Demand for Criteria

Criticality criteria are often used to identify and rank infrastructures in order to establish inventories, risk registers, and

* E-mail: alexander.fekete@bbk.bund.de

protection priorities (Moteff 2004; Swiss Federal Office for Civil Protection 2009). Criticality criteria also have been reviewed (Theoharidou, Kotzanikolaou, and Gritzalis 2009) for specific aspects such as interdependency dimensions (Rinaldi, Peerenboom, and Kelly 2001; de Porcellinis et al. 2009). But common criteria for the identification of "critical infrastructures" and structured concepts for criticality analyses are wanting. One reason is the confusion between key terms: risk, vulnerability, resilience, and criticality. Concepts and criteria for the identification of critical infrastructures vary wildly and at random use criteria typically employed in impact assessments, social vulnerability and economic damage assessments, capacity, capability and resilience studies, and other general risk parameters such as probability and damage extent. Although there are efforts to structure and identify the different approaches, for instance regarding systemic failures, consequences of failures, single-hazards, or all-hazard approaches (JRC/IPSC/TRVA 2007; Bonin, Doktor, and Habegger 2009), the difference between criticality and other risk-terms is not clear. In most cases, infrastructure criticality assessment is just another wording for risk, vulnerability, or resilience assessment of infrastructures. The differences in terminology could be just an academic curiosity. Nonetheless, the quest for standardized approaches is important for the cross-country analyses that are currently being carried out by the EC (EC 2008).

This paper investigates simplified patterns valid for many infrastructures and infrastructure assessments. The objective is less to provide fundamentally new insights, and more to extract what are essential and common features that are typical for criticality. The paper starts with a conceptual discussion of the terms critical and criticality. Then criteria are described that can be used to measure criticality generally for most types of infrastructure.

2 What is Critical and What is an Infrastructure?

Critical infrastructures are infrastructures regarded as especially important for society. But what does "critical" mean and what defines whether the infrastructures are merely important as opposed to especially important? What are infrastructures and their components? These questions have to be answered before going deeper into the assessment of infrastructures.

2.1 What is "Critical"?

The etymology of the term "critical" is strongly related to the concept of crisis and points to a crucial or decisive characteristic, situation, turning point, or impending change (see, for example, Online Etymology Dictionary 2010; Merriam-Webster Dictionary Online 2010). This section combines the various uses of the term critical in the context of infrastructure and identifies common essential features. This is done by determining which criteria can be used to describe what makes an infrastructure or its features critical.

Analysis of the most common uses of the term critical in the critical infrastructure literature reveals two aspects: first, relevance; and second, risk. Relevance is indicated when a certain infrastructure is important for a large proportion of society. Risk occurs when the infrastructure becomes a threat to the community, for example, by not supplying the population anymore. Many infrastructures are important, but only when they reach a certain critical threshold (size, relevance, or brittleness) is their criticality revealed. In a nutshell, criticality points to relevance at a threshold. For instance, criticality is very often defined as a type of significance revealed by the negative impacts of an outage (Federal Ministry of the Interior of Germany 2009; EC 2008).

The overall criticality of a given object of interest is related to two temporal phases of investigation: the object's normal operation characteristics and its characteristics in case of a failure. Criticality, therefore, describes the relevance of a given asset, which can be described by capabilities such as load, or indirectly by the number of customers supplied with a product or service. This relevance is, however, critical at a certain decisive moment, here in the case of failure, when suddenly the service provided by the object is interrupted.

2.2 Ways to Describe Criticality

There are at least two big questions behind the criticality of infrastructures: On what are we dependent? What would be the impacts of failure? Some studies use criticality assessment as a preliminary step toward identification of priority areas, and later merge into a more detailed analysis of hazards, vulnerabilities, and risk (Federal Ministry of the Interior of Germany 2007). Most approaches identify risk elements or processes that carry large supply capacities. Some studies regard certain infrastructures as critical, or important, even vital (Luiijf, Burger, and Klaver 2003), irrespective of any imaginable impact.

Many studies that deal with infrastructure criteria, however, use consequence-based criteria to connect the supply capacities of infrastructures with impact scenarios of potential damage (EC 2008; Theoharidou, Kotzanikolaou, and Gritzalis 2009). There are numerous impact types, such as mortality, harmed people, economic damage, and image loss, among others. Impacts help direct the assessment towards the interests of the researchers. For example, for the task of a civil protection agency, the focus on human lives should be paramount.

There are at least three ways to describe criticality:

(1) Criticality might be described by regarding the internal relevance of an infrastructure, in short the maximum loss of service capability possible. This is the internal system capability;
(2) Alternatively, the external impacts can be described, for example, the number of customers supplied; and

(3) Criticality can also be described by the decisive capabilities needed to prevent, mitigate, or compensate for failures due to infrastructure impairment, for instance the 4Rs of resilience: robustness, redundancies, resourcefulness, and rapidity of Tierney and Bruneau (2007).

2.3 What is an Infrastructure?

An infrastructure is a structure utilized by humans for the provision of services and goods. Definitions for infrastructures, and specifically so-called critical infrastructures, can be found in international handbooks (Brunner and Suter 2008) and are officially defined for countries such as Germany (Federal Ministry of the Interior of Germany 2009). Natural or human-environmental structures such as rivers are infrastructures as are technical structures such as pipelines. But infrastructures consist of components both visible and invisible. Infrastructures contain systemic and spatial features (Bouchon 2006), yet they also possess more organizational and other less visible facets. As an example for nontechnical infrastructure features, human staff is (often) crucial for creation, management, and maintenance or repair of infrastructures. Moreover, functions and processes, such as organizational processes, laws and regulations, and a great variety of quality aspects, are all components that are indispensable for the functioning of infrastructure services. For example, the critical component of the infrastructure finance system might be trust rather than a certain technical asset. Lastly, the environment and the so-called environmental services, such as natural resources, are essential components of many infrastructures.

The following table shows a conceptual list of infrastructure components, deduced by a cross-sectoral analysis of the official critical infrastructure (KRITIS) sectors used by Germany's Federal Ministry of the Interior and the Federal Office of Civil Protection and Disaster Assistance. This conceptual consideration is also based on review of scientific literature and on both unclassified and classified documents by governmental agencies. Examples are provided for four component areas. The major purpose of Table 1 is to extend the focus from technical infrastructures to features such as human staff, various processes summarized as functions, and the environment in which the infrastructure stands and from which it takes its resources. The examples in Table 1 illustrate different types and characteristics of the respective infrastructure components. The components as well as the examples are not exhaustive and strive to construct a more holistic concept of infrastructure as compared to a purely technical comprehension of infrastructure.

Table 1. Infrastructure components

Technical structures/ assets	Human staff	Functions	Environment
Nodes Linear or network structures	Staff in: Planning Management Maintenance Repair	Organization Processes Quality Regulations	Environmental services Natural resources Spatial setting

2.4 Specific Aspects of a Criticality Assessment

The concept behind a criticality assessment is similar to a typical risk assessment. Especially for assessments of critical infrastructures, however, certain adjustments are typical:

(1) Only impacts due to infrastructure impairment or failure are considered, not direct impacts of hazards such as human staff killed by lightning;
(2) External effects outside the hazard of place are important. For example, a flood in region x can affect the energy supply in region y; and
(3) Interdependencies and cascading effects leading to different impact entry-points must be evaluated.

The viewpoint of some national critical infrastructure protection programs (Federal Ministry of the Interior of Germany 2007) requires a focus on the consequences specifically due to the service failure of an infrastructure. The focus lies on mortality, economic loss, or other negative outcomes directly related to service interruption of infrastructures. In some cases, the hazardous aspects of certain infrastructure such as nuclear power plants, or the risks due to the failure of certain protection infrastructures such as flood walls or levees, are not considered. There exist political or administrative reasons for this position and, sometimes, there is a lack of resources to cover all aspects related to infrastructure risks.

Hazards can be internal or external to the infrastructure system. The all-hazard approach requires a concept that can be applied to all sorts of hazards, be they naturally induced, human derived, technology based, or any combination of these. Even more, hazards and interruptions of infrastructure can happen in remote regions and still impact the given infrastructure system or sector of interest. Examples are interruptions of the World Wide Web, the effects of the ash from a volcano in Iceland on air traffic in Europe, and blackouts of the power grid originating in one country and affecting other countries.

Infrastructures are linked together and the failure of one infrastructure, for instance the power grid, affects a wide range of other infrastructures, for example water supply and information technology. Criticality assessment needs to determine the consequences and damages of such interdependencies (Rinaldi, Peerenboom, and Kelly 2001). For the full picture on failure, it is necessary to capture second and third order consequences as well.

Finally, criticality assessment often faces many uncertainties and limitations on access to data and information. Many assumptions and simplifications have to be made. For example, assuming complete failure of one element or node helps understanding of the importance of that one node for

the whole system. In a typical risk or vulnerability assessment, all existing protection and mitigation measures would be considered, as well as the plausibility of failure due to one specific hazard. This is valid for a detailed risk analysis, but hampers the identification of the relative importance of infrastructure elements. Moreover, the surprise factor of unexpected new hazards or the unexpected extent of known hazards would be overlooked. The same is true for safety preparedness or measures regarded as sufficient for given scenarios.

3 Common Properties of Criticality Criteria

Criticality is used in nuclear science to describe the conditions necessary to produce a chain reaction. While a certain critical mass of uranium is necessary, also the temporal aspects and the quality of the enriched uranium, the heavy water, and other conditions all contribute to a successful chain reaction. Criticality, it is hypothesized, can be described by three general characteristics:

- Critical proportion
- Critical time
- Critical quality

3.1 Critical Proportion

Critical proportion summarizes many aspects commonly denoted as most important in the assessment literature. Critical proportion contains aspects such as the critical number of elements or nodes of an infrastructure (USDHS 2003, viii), choke points (USDHS 2006, 127), as well as critical number of services, size of population (Theoharidou, Kotzanikolaou, and Gritzalis 2009, 42), or magnitude of customers affected. In many cases the criterion might better be described by percentages or proportions rather than absolute values. Moreover, other aspects such as the critical spatial extent, outreach, scope (Theoharidou, Kotzanikolaou, and Gritzalis 2009, 39), or population density can be expressed with this criterion. It also captures criteria often sought to describe capacities for preparedness, response, or recovery, such as the number of redundancies, buffers, or other aspects of resilience (Tierney and Bruneau 2007); the same criterion may well describe the number of interdependencies involved (Rinaldi, Peerenboom, and Kelly 2001). All aspects of criticality point to a certain threshold that, when crossed, starts to seriously affect an infrastructure system upon which depend other infrastructures or populations. The critical proportion can also be inverse. For example, certain very rare or specialized items such as rare earths exist in limited amounts, yet, their outreach and importance for the world market can be very high.

Many sources dealing with criticality of infrastructures use impact criteria such as number of casualties, injured people, or economic damage (EC 2008). They all point to the same criterion, a critical proportion, expressed by different types of measurable impact. The critical proportion criterion has limited ability to capture nonquantifiable aspects, such as processes or other soft issues. This is an important issue to consider, since many experts, especially from the private sector, promote looking at organizational processes rather than specific products or elements. As soon as one process is identified as critical for the whole service delivery by one particular infrastructure, a deeper investigation will start to analyze which parts of the process make it critical. Here the critical proportion is a useful criterion especially as it is often easier to visualize physical elements, including human staff, that compose the processes. But less visible and countable elements of infrastructures are often key to understand criticality. At this stage, other criteria such as time or quality can be more useful.

3.2 Critical Time

Critical time summarizes aspects such as duration of outage, speed of onset, and specific critical time frames, but also notes the capacities before, during, and after a crisis. The latter are, for example, Mean Time to Repair (MTTR), Mean Time to Recovery, Mean Time to Functionality (MTTF), and business continuity or interruption. Critical time covers not only on/off, yes/no cases but also gradual transitions. For instance, resilience, as an inherent feature of systems, includes temporal aspects such as change, in addition to the characteristic to "degrade gracefully when it must" (Allenby and Fink 2005, 1034). Resilience in respect to threat and hazard features is by some sources (Kahan, Allen, and George 2009, 15) "characterized principally by time and not necessarily by geography or spatial location." Adopting the resilience approach to criticality, temporal characteristics can be just as important as physical nodes or spatial location, not only regarding threats but also system robustness or emergency capacities. Combining the criticality of an element or spatial extent of a failure with a temporal criticality characteristic enhances the criticality assessment. For gradual temporal transitions, however, the critical tipping point (Gladwell 2000), or threshold of criticality, is often difficult to determine.

In many cases, the real scale of a disaster can only be captured by investigating the duration an outage or impact lasts. For example, the 2006 blackout cascading all over Europe affected several countries, but only for less than one hour. But what if it had lasted for days? Another example is the ash cloud produced by the Icelandic volcano Eyjafjallajökull. The eruptions interrupted international air traffic and left more than one million passengers on the ground (Chittenden and Swinford 2010). More research is needed to determine how close certain industries have been to serious business interruptions; some car manufacturers in Germany already had to reduce production. But what if the eruption had lasted 13

or 14 months as was the case the last time Eyjafjallajökull erupted in 1821?

Other than duration, the timing of an impacting event can be critical. For example, public administration authorities are often difficult to describe as critical due to a distinct duration of failure. Were a failure to occur on the day when all the transactions for wages or benefits were due, however, the effects would be far more tremendous than during the rest of the month. Another example is public buildings or train stations during service hours or other public buildings such as conference halls. Most of the year a harmful event would cause no harm, but when many people or, for instance, all shareholders and managers of a company meet, this would be a critical, disruptive timing.

3.3 Critical Quality

Critical quality summarizes aspects such as the quality of the service delivered (for example water quality), and includes public trust in (water) quality. One recent example is the case of food poisoning in Europe. By June 8, a strain of *Escherichia coli* had sickened over 2400 people in Germany and caused 24 deaths (Peter 2011). Raw vegetables, such as tomatoes, lettuce, and cucumbers, and later on bean sprouts, were suspected to be the source of the bacteria. This suspicion resulted in a sharp decline in the consumption of these vegetables, due in part to the precautionary advice by the European Commission and German health authorities. While the link of the infections to the vegetables remains uncertain, economic loss among European vegetable producers is high (Peter 2011). The lack of quality or the loss of consumer trust in a product or service is a critical criterion that links infrastructure services to mortality, economic loss, or other unwanted outcome.

The critical quality criterion captures also loss of trust in authorities, image loss of companies, and impacts on core values (Metzger 2004, 76). A lack of quality might seriously disturb the usability of the service delivered by infrastructures. Even when the technical structures, human personnel, and administrative organization are all in place and still delivering the good or service, it might be of no use because of lack of quality—whether that deficiency is real or only perceived. Quality includes identity and ethics and therefore highlights organizational processes that are the baseline for ensuring the integrity and operability of infrastructure services.

3.4 Generic Criticality Types of Infrastructure for a Quick-Scan

The combination of infrastructure components (Table 1) with criticality criteria allows construction of preliminary criticality types of infrastructures. Most of these are at least implicitly researched in many studies so that they might be described as typical or generic. Infrastructures are analyzed within physical, systemic, and spatial taxonomies (Bouchon 2006, 23). They can be extended to incorporate temporal aspects. Generic criticality types for a quick-scan might be:

Generic physical/spatial criticality types

- Point types: single points of failure (SPOF) / choke points / nodes / (national) icons
- Line types: linear connections / cascades / transfer stations / limited connectivity paths / linear networks
- Area types: mass item / viral distribution / non-linear networks / cloud-computing

Generic temporal criticality types

- Quick onset types: impact realization on human life or system functionality
- Slow onset types: failure duration, MTTR
- Time slot type: time delay, specific time frames, tipping points, “critical situations”

The use of criticality types helps determine what to identify as critical. The problem is that almost all assets of an infrastructure can become critical, if the proportion, time, or quality cross a certain threshold. Since this threshold is hard to determine, especially for nonlinear and interwoven infrastructure systems, it is practical to have imprecise but fit-all types at hand for a quick-scan and first assessment.

For the establishment of priority lists, the collection of single points of failure (SPOF) is important and useful for a quick-scan assessment. The relevance of unique, rare or specialized assets is obvious and the related redundancy question is a key feature of Critical Infrastructure Protection (CIP) concepts (Federal Ministry of the Interior of Germany 2007; JRC/IPSC/TRVA 2007, 20; German Advisory Council on Global Change 2000, 288). The opposite extreme to SPOFs, mass items, can also become critical when their quality is compromised or their network layout is exploited, for instance by malicious attacks using the internet or generally Information Technology (IT). Especially in the example of the internet it becomes evident that the network character, with a great many redundancies and decentralized servers, is by its nature very susceptible to viral types of hazards such as intentional attacks. Cyber crime exploits the decentralized, internationalized, and externalized structure of the network. This has major implications for a characteristic that is generally believed to increase failure tolerance: decentralization (Perrow 1999). Centralization/decentralization would be another generic criticality type to examine in order to develop measures that reduce criticality. As with all generic criticality types described here, there is no black and white distinction—all types are characterized by a high degree of ambiguity. For example, SPOFs are easy targets, but are at the same time predestined to receive priority security measures.

For infrastructure components that are less related to physical or spatial settings (Table 1) generic types can be found. For example, interdependencies in terms of the types of relation are differentiated as cyber, logical (Rinaldi, Peerenboom, and Kelly 2001), or societal (de Porcellinis et al. 2009). Other sources discuss types of systems or functional components and their different use within systemic or spatial approaches (Bouchon 2006, 20, 23).

Infrastructures are not critical merely at nodes or hot spots. Pipelines and power poles can also become critical if the critical amount of affected assets is high enough. For instance, several power poles failed during a 2005 winter storm in Germany, leading to blackouts lasting up to seven days in some villages. As another example, the viral distribution of malware or denial of service attacks makes use of mass items such as telecommunication lines, servers, or personal computers. A network may not go down when certain nodes fail, but only when a larger, critical proportion of the network fails. While line and network features have other risk characteristics as compared to point features, all of them can become critical in their specific ways and should not be excluded from an assessment.

4 An Application Example

Application areas that make use of generic criteria and a deeper conceptual understanding of what critical means in combination with infrastructure are found in research, risk management, and politics among other areas. Research benefits from a conceptual debate about how to define criticality and how to measure it as well as from the results of case studies. But case studies of critical infrastructure often lack a theoretical framework and might benefit from a more holistic understanding. Risk management concepts employed by business, public administration, and nongovernmental organizations (NGOs) in the development arena also benefit from the extension of conceptual paradigms, but are more closely linked to the decision maker's question: where do I need to focus my attention? CIP analyses often seek to identify priority areas for further risk management in order to reduce effort and costs. Risk assessments are often a key aid in the identification of risk hot spots, and in many aspects criticality assessments are very similar. In principle there are multiple ways to conduct such assessments: top-down or bottom-up, sector-specific or cross-sectoral, and so forth. The objectives of the researchers, risk managers, and decision makers all influence the choice of method, concept, and application of a criticality assessment of infrastructures. Therefore there are various possibilities for application and the following sections provide only an example of how to derive applicable specific criteria from the common criteria presented in the previous sections. The example demonstrates how these criteria are used for an assessment of critical infrastructures by the Federal Office of Civil Protection and Disaster Assistance in Germany.

4.1 Operationalization of the Criteria

A good common definition must be so broad and general that it can be applied for different uses, in this instance for different types of risk analysis or different types of infrastructure. Broad and general definitions are often difficult to use. Frequently definitions and conceptual frameworks must be adapted and made more explicit. The same is true for the common criteria of criticality as described in the previous section. These common factors (critical proportion, time, and quality) integrate many typical characteristics of critical infrastructures and provide ideas for the development of specific criteria. Table 2 contains a nonexhaustive list of possible examples of such criteria that result from a cross-sectoral and interdepartmental analysis of CIP literature, various case studies, and expertise on individual infrastructure sectors.

Table 2 contains criteria that can be derived from the three generic criteria and criticality types in section 3. Many of the examples are criteria typically applied in studies on critical infrastructures. Table 3 uses two general aspects of criticality assessments as described in section 2.2—the criticality within a system, and the criticality for society. The criticality within a system, described by the internal infrastructure capabilities are, for example, the chain reactions resulting from the failure of a critical node or asset, and the capabilities to mitigate such failures. The criticality for society, in this case, the civil protection impact dimensions, is captured by two aspects,

Table 2. Nonexhaustive criteria for various infrastructure types

Generic criterion	Examples of specific criteria	Examples of applications (many criteria are valid for almost all types of infrastructure)
Critical proportion	Load, capacity, power, sales, turnover, etc.	Traffic, logistics chains, power installed
	Number of assets, nodes, interdependencies, redundancies, emergency capacities	Backup systems for power or information storage; emergency power
	Amount of customers supplied	For instance, the number of people supplied with drinking water
	Outreach / spatial interconnectedness	The single chemical plant in the world producing a key product
Critical time	Failure duration	Air traffic grounding due to volcanic ash
	Mean time to repair, replace, restore the functionality	Replacement time for a transformer station
	Mean time to react	Police, fire brigade, medical units, media, early warning, crisis management
	Timing of failure	Coldest winter day; annual meeting of company leaders; day of distribution of welfare or pay checks
Critical quality	Product or service quality	Water or food quality, trust in finance, training of staff, feeling of security
	Cultural or societal significance	National cultural icons

Table 3. A typical national critical infrastructure priority list for civil protection

	Top 10 suppliers (for example by market share)				**National icons / rare yet important key services or elements**			
Infrastructure capability								
Sector A	1	2	3	…	1	2	3	…
Sector B								
…								
Civil protection impact dimensions								
Critical proportion / impact extent	Sub-national		National		Sub-national		National	
Number of people supplied (by A1, A2, … B1, etc.)	International		Global		International		Global	
Critical time Impact realization = speed of onset to impact human life or health	X minutes, hours, days …				X minutes, hours, days …			

the number of people supplied by infrastructure services per regional unit and the critical time, the speed of onset to affect human life or health. The columns of Table 3 capture only a limited selection of the three generic criteria of section 3 or the more specific examples in Table 2. Two key aspects of critical proportion are termed "top 10 suppliers" and "national icons / rare yet important key services or elements" (Table 3). These two key aspects are selected for their importance and rather intuitive comprehension by the users. Table 3 can be used to investigate several infrastructure sectors.

Table 3 does not intend to suggest that other criticality criteria should not be considered. Specifically, other aspects of proportion, temporal, and quality aspects must complement a thorough investigation of the criticality of infrastructures. In the following a simplified example of distinct criticality criteria is given which would typically be used to establish a national critical infrastructure inventory or priority list. Please note that this list is not related to a real case and the criteria are only examples, and not exhaustive.

Table 3 shows a quite intuitive and accessible way to condense the complex set of possible criticality criteria. The idea is to start in a top-down approach with the biggest infrastructures per country. The biggest infrastructures are those with the largest service output, production rate, or market share. Additionally, the most iconic or special infrastructures are collected, such as national monuments; also included are unique items such as the parliament. Very specialized and outstanding infrastructures with a distinct quality are collected here that may be rather unknown to the public but are world-wide market leaders of specific products or services. This national inventory is further filtered according to impacts on the population, which is the main scope of civil protection. The number of people affected, the spatial and international impact dimension, and temporal criticality factors are used here. Precise numbers are often difficult to assess. Alternatively, classes of coarse dimensions can be used, for instance, the differentiation of minutes, hours, or days of impact. Not all impact criteria must be provided, but it is recommended to use at least one. The more impact filter criteria are used the more precise the outcome will be. On the other hand, comparability with other infrastructure sectors will typically be hampered by data constraints. In principle, the link between infrastructure capabilities and civil protection impact dimensions is useful for identifying civil protection priorities on national, municipal, or household level.

There are obvious limitations in this simplified example. For example, Table 3 showcases a typical national inventory in a top-down approach. For the assessment of critical elements within a given infrastructure system, and especially on other spatial scales, other criteria and observation levels are necessary. For instance, inventory lists, but also criticality assessments in general, might look not just at the biggest or most iconic components but also at the weakest links, hubs, limits of emergency capacities, dependencies, and interdependencies. Integrative and multi-level or participatory approaches might be considered to test, complement, or even replace the often one-sided and limited knowledge created by top-down approaches such as the one presented in Table 3. For example, bottom-up approaches and in-depth local studies are indispensable for precise data mining, for understanding the impact of failures on local households, and for risk analyses of concrete infrastructure components.

4.2 Demand for Criticality Criteria within National Civil Protection in Germany

Criticality assessment using the criteria and the concepts outlined here is used by the Federal Office of Civil Protection and Disaster Assistance (BBK) in Germany in order to derive priority infrastructures. Those infrastructures identified are

relevant to the extent that their failure would result in intolerable effects for the public. The goal of the BBK is to preserve the well-being of the population in terms of the supply of services delivered by infrastructures.

Full protection against all threats and cascading effects is not financially viable for society (Apostolakis and Lemon 2005, 361) and may not even be feasible. In the recent disaster risk discourse, alternative strategies have to be explored, such as vulnerability, resilience (Lovins and Lovins 1982), and their specific recent branches such as societal risk (Bonin, Doktor, and Habegger 2009) or community resilience (Boin and McConnell 2007, 54). Against a backdrop of unlimited failure and impact possibilities for all kinds of infrastructure services or sectors, a prioritization of critical elements, security measures (Lauwe 2010), and vulnerabilities (Apostolakis and Lemon 2005, 361; Moteff 2004; Swiss Federal Office for Civil Protection 2009) is necessary.

For this purpose, the project KritisKAT is developing a concept for the cross-sectoral identification, evaluation, and comparability of critical infrastructures in an all-hazard approach. Criticality assessment is a corner stone of the risk assessment of infrastructures methodology of the BBK (Federal Ministry of the Interior of Germany 2007). KritisKAT implements actions of the German CIP strategy (Federal Ministry of the Interior of Germany 2009) and provides a concept for the criticality assessments carried out on national level and in collaboration with federal states, municipalities, and the private sector. The infrastructures that are investigated in KritisKAT are the respective critical infrastructure sectors that are defined by the Ministry of the Interior and used by the BBK (Federal Ministry of the Interior of Germany 2009). The internal list of critical infrastructures has just been updated and now includes energy, information technology and telecommunications, transport and traffic, health, water, food, finance and insurance industry, government and public administration, and media and culture.

Project KritisKAT's goals are the identification of critical infrastructure elements and an assessment of impacts on society due to service interruptions in order to derive a preselection of infrastructure sectors and branches for future risk analyses and risk management actions in civil protection. Deliverables are criticality criteria useful for an integrative, cross-sectoral, interdepartmental, and standardized concept for criticality assessment. The results of project KritisKAT will be used to consider a national inventory of critical components, to conduct risk analyses, and to outline risk management actions. The results of KritisKAT will foster the development of both strategic and operational civil protection goals regarding the interplay between critical infrastructures and society.

The KritisKAT project fosters cross-sectoral and interinstitutional collaboration within the federal office and with other public authorities and the private sector. It triggers other research such as a macroeconomic input-output analysis and societal risk goals. Project KritisKapa, a spin off from the work within the BBK and KritisKAT, will assess emergency capacities in the energy sector and possible thresholds for societal risk goals concerning civil protection. Thresholds of capacities on several levels—operator, civil protection, public authorities, and the population—are promising critical tipping points, useful for the development of societal risk goals. The outcome of KritisKAT will be used not only to frame recommendations for public authorities and private operators of infrastructures, but also to establish risk communication with civil society.

5 Conclusions

The main results of this paper are conceptual insights into what is critical and what constitutes infrastructures. Critical are nodes or hot spots. But also very important are line features and mass items. Networks and decentralized systems can also reach thresholds where impacts such as impairment or failure become intolerable for society. As another finding of this paper, infrastructure is more than just technical lines or physical assets—hardware. Temporal characteristics are paramount for identifying what makes infrastructures critical. Other soft issues such as organizational processes or even product quality also determine risks to and by infrastructures.

This paper has outlined key characteristics and objectives of a criticality assessment—infrastructure components, both visible and invisible—established common criticality criteria, and presented an example of how such generic criteria can be used in practical ways. The generic criteria and the specific operational criteria presented in this paper do not represent a directly applicable or exhaustive list of criteria for a specific assessment. As with most conceptual papers the emphasis lies in conveying general ideas that in later steps can be employed for assessments. The criticality assessment as described in this example formulates an elaborated hypothesis of what might potentially become critical. Such a criticality assessment does not replace a thorough investigation of hazards, or any concise vulnerability, resilience, or risk assessment of system components.

The three criticality criteria outlined in this paper can be applied to a wide range of different infrastructures in order to elicit the aspect(s) that makes them critical. There are two distinct reasons to suggest the utility of these general criteria despite the plethora of criteria already available in the literature: (1) they identify common denominators valid within most of the approaches that identify and rank criticality. This simplifies and reduces the confusing array of factors and provides reasonable coherence to analysis; and (2) they reveal criteria or subcriteria not considered yet in some approaches in literature. Examples are the variety of temporal aspects that constitute a critical threshold, or quality in all its various forms, which is often not considered, as well as most invisible features of technical infrastructures.

Limitations of this paper exist both conceptually and in application since the described common criteria, infrastructure components, and application are merely examples. The critical infrastructure approach does integrate many similar approaches to infrastructures. At the same time, this is not the only way to structure and conceptualize critical infrastructure. Likewise, this paper presents only a top-down type of assessment and application. Bottom-up approaches and other alternative approaches to infrastructure resilience might be another future issue to apply, test, and amend the proposed generic criticality criteria and infrastructure components. The paper does not debate the similarities and differences of criticality to vulnerability or resilience concepts. This might be a topic for future investigation.

This concept and the criteria emphasize a focus on society and set the stage for the future development of societal risk goals. The focus of civil protection should be on society not on technical elements or processes within an infrastructure. Ultimately, it does not matter in respect to civil protection what the exact defect in an infrastructure is; it matters how people are affected.

Acknowledgments

The author wishes to express his gratitude to the anonymous reviewers for the opportunity to profit from the thoughtful and constructive comments. The author is grateful for the information and constructive feedback provided by the risk academy and parallel session during the IDRC 2010 conference in Davos, the participants at the Cap-Haz Net meeting in Haigerloch, Germany 2010 as well as for intense discussions with the colleagues at BBK. The author wishes generally to emphasize that he is indebted to many ideas raised by other literature sources and informal talks with fellow researchers, apologizes for being unaware of similar research results and publications that are outside his range of knowledge, and is grateful for further reading suggestions.

References

Allenby, B., and J. Fink. 2005. Toward Inherently Secure and Resilient Societies. *Science* 309 (5737): 1034–36.

Apostolakis, G. E., and D. M. Lemon. 2005. A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. *Risk Analysis* 25 (2): 361–76.

Australian Government. 2010. *Critical Infrastructure Resilience Strategy*. Commonwealth of Australia. http://www.tisn.gov.au/.

Boin, A., and A. McConnell. 2007. Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management* 1 (15): 50–59.

Bonin, S., C. Doktor, and B. Habegger. 2009. *Risk Analysis. Integrated Risk Management and Societal Security. Focal Report 2*. Center for Security Studies, ETH Zürich.

Bouchon, S. 2006. *The Vulnerability of Interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-Art*. Institute for the Protection and Security of the Citizen, Joint Research Centre, European Commission.

Brunner, E. M., and M. Suter. 2008. *International CIIP Handbook 2008/2009*. Center for Security Studies, ETH Zurich.

Chittenden, M., and S. Swinford. 2010. Volcanic Ash Grounds Britain for Days to Come. *Times Online*. April 18. http://www.timesonline.co.uk.

EC (European Commission). 2008. *COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection*. Official Journal of the European Union. 23.12.2008. L 345/75-82. http://eur-lex.europa.eu/JOIndex.do.

Federal Ministry of the Interior of Germany. 2007. *Protecting Critical Infrastructures—Risk and Crisis Management. A Guide for Companies and Government Authorities*. Berlin.

——. 2009. *National Strategy for Critical Infrastructure Protection* (CIP Strategy). Berlin.

German Advisory Council on Global Change. 2000. World in Transition. *Annual Report 1998*. Berlin: Springer.

Gladwell, M. 2000. *The Tipping Point: How Little Things Can Make a Big Difference*. New York: Back Bay Books.

JRC (Joint Research Centre of the European Commission). 2007. *Towards the Definition of Criticality Criteria for the Identification of European Critical Infrastructures*. Ispra.

Kahan, J. H., A. C. Allen, and J. K. George. 2009. An Operational Framework for Resilience. *Journal of Homeland Security and Emergency Management* 6 (1): 1–48 (Article 83). http://www.bepress.com/jhsem/vol6/iss1/83.

Lauwe, P. 2010. The Protection of Critical Infrastructure within Germany. In *Toward A Grand Strategy Against Terrorism*, edited by C. C. Harmon, A. N. Pratt, and S. Gorka, 328–40. New York: McGraw-Hill.

Lovins, A. B., and L. H. Lovins. 1982. *Brittle Power. Energy Strategy for National Security*. Andover, Massachusetts: Brick House Publishing Co.

Luiijf, E. A. M., H. H. Burger, and M. H. A. Klaver. 2003. Critical Infrastructure Protection in The Netherlands: A Quick-scan. In *EICAR Conference Best Paper Proceedings*, edited by U. E. Gattiker, 19 pages. Copenhagen: EICAR.

Merriam-Webster Dictionary Online. 2010. Accessed November 24. http://www.merriam-webster.com/dictionary/critical.

Metzger, J. 2004. Challenging the Concept "Critical Infrastructure Protection" (Das Konzept "Schutz kritischer Infrastrukturen" hinterfragt). *Bulletin 2004 zur schweizerischen Sicherheitspolitik*, 73–85.

Moteff, J. 2004. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*. [Washington, DC]: Congressional Research Service, Library of Congress. http://www.ndu.edu/library/docs/crs%209.07.04.pdf.

——. 2007. *Critical Infrastructure: The National Asset Database*. [Washington, DC]: Congressional Research Service, Library of Congress.

Online Etymology Dictionary. 2010. Accessed November 24. http://www.etymonline.com/index.php?search=critical&searchmode=none.

PEP (Provincial Emergency Program). 2007. *Critical Infrastructure Rating Workbook*. Provincial Emergency Program, British Columbia, Canada.

Peter, L. 2011. E. coli: EU Vegetable Producers Hit Hard. *BBC News*. June 28. http://www.bbc.co.uk/news/world-europe-13698760.

Perrow, C. 1999. *Normal Accidents: Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press.

de Porcellinis, S., G. Oliva, S. Panzieri, and R. Setola. 2009. A Holistic-Reductionistic Approach for Modeling Interdependencies. In *Critical Infrastructure Protection III*. Proceedings. Third Annual IFIP (International Federation for Information Processing) WG 11.10 International Conference on Critical Infrastructure Protection. Hanover, New Hampshire, USA, March 23–25, 2009: revised

selected papers, edited by C. Palmer and S. Shenoi, 215–227. Berlin: Springer.

Rinaldi, S. M., J. P. Peerenboom, and T. K. Kelly. 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine* 21 (6): 11–25.

Robert, B, M.-H. Senay, M.-È. P. Plamondon, and J.-P. Sabourin. 2003. *Characterization and Ranking of Links Connecting Life Support* Networks. Ottawa: Public Safety and Emergency Preparedness Canada.

Swiss Federal Office for Civil Protection. 2009. *The Swiss Programme on Critical Infrastructure Protection*. Federal Office for Civil Protection. Bern.

Theoharidou, M., P. Kotzanikolaou, and D. Gritzalis. 2009. Risk-Based Criticality Analysis.In *Critical Infrastructure Protection III*. Proceedings. Third Annual IFIP (International Federation for Information Processing) WG 11.10 International Conference on Critical Infrastructure Protection. Hanover, New Hampshire, USA, March 23–25, 2009: revised selected papers, edited by C. Palmer and S. Shenoi, 35–49. Berlin: Springer.

Tierney, K., and M. Bruneau. 2007. Conceptualizing and Measuring Resilience. A Key to Disaster Loss Reduction. *TR News* 250: 14–17.

UKCO (United Kingdom. Cabinet Office). 2010. *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*. London.

USDHS (United States. Department of Homeland Security). 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC: [Department of Homeland Security].

——. 2006. *National Infrastructure Protection Plan*. [Washington, DC]: Department of Homeland Security.

Vrijling, J. K. (Han), P. H. A. J. M. van Gelder, L. H. J. Goossens, H. G. Voortman, and M. D. Pandey. 2004. A Framework for Risk Criteria for Critical Infrastructures: Fundamentals and Case Studies in the Netherlands. *Journal of Risk Research* 7 (6): 569–79.