TRENDS IN CRITICAL INFRASTRUCTURE PROTECTION IN GERMANY

Christine EISMANN[1]

Review article

Abstract: Critical Infrastructures failures cause harmful consequences to the population, because they disrupt the supply of necessary goods and services. The failures pose an indirect threat, as they will regularly be triggered by natural hazards, technical failure/human error or intentional acts. In the risk analyses on the national level in Germany, Critical Infrastructure failures are qualitatively described to estimate their impacts on society. Critical Infrastructure Protection is seen as a joint task of many different stakeholders. Rules and regulations with different degrees of compulsion build the framework for their cooperation, and a strategy is in place that promotes the trustful exchange of information among all the relevant stakeholders. The most important stakeholder groups are public authorities, infrastructure operators, and the population. An example is given on how a joint risk management of public authorities and infrastructure operators may be performed, and the cooperation of public authorities and the population is discussed. As Civil Protection covers the entire risk and crisis management cycle with its phases prevention, preparedness, response and recovery, the article ends with examples of the support, which the German Federal Office of Civil Protection and Disaster Assistance and the Federal Ministry of the Interior offer for other stakeholders in order to achieve well-protected infrastructures and, in consequence, well-protected citizens.

Keywords: Civil Protection, Critical Infrastructures, Germany, risk management, crisis management.

Introduction

This article corresponds with the presentation given at the Brokerage Event 2014, Development and Application of New Trends in Public Safety, Security and Protection, on 7 October 2014 in Ostrava, which was hosted by the Moravian-Silesian Region, the Regional Development Agency, the Moravian-Silesian Regional Fire Rescue Service, the VŠB-Technical University of Ostrava - Faculty of Safety Engineering, and the Safety & Security Technology Cluster.

In the article, the role that Critical Infrastructures play in the German civil protection system will be discussed. Starting from their definition and the sectors, it will be shown why they take up a special status, which stakeholders are needed for their protection and how they can be integrated in a protection system that follows the risk and crisis management cycle.

Materials and methods

Critical Infrastructures in Germany

In Germany, Critical Infrastructures (CIs) 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" (German Federal Ministry of the Interior, 2009). Nine sectors have been identified critical on the national level. These are:

- Energy/power supply,
- Information and communications technology,
- Transport and logistics,
- (Drinking-) water supply and sewage disposal,
- Public health/medical services,
- Food,

[1] German Federal Office of Civil Protection and Disaster Assistance (BBK), Bonn, Germany, christine.eismann@bbk.bund.de

DOI 10.2478/tvsbses-2014-0008

- Public administration, including emergency and rescue services,
- Economic services/finance, insurance business, and
- Media and cultural objects (cultural heritage items).

The definition and also the sectors show that the main focus is clearly on the disruption of supplies and services. Infrastructures, in which dangerous substances are handled such as chemical industry factories or nuclear waste sites, are, for example, not addressed in the definition. This is interesting to note, as some European countries have a wider definition in place.

The infrastructures under consideration are those, whose failure can lead to an effect on the population or on other infrastructures. A threat or scenario - e. g. a storm - can therefore influence the population in a threefold way (see Fig. 1). First, it can have a direct impact on the population, such as causing injuries if people are outdoors. Second, it can lead to Critical Infrastructure failure, e. g. electricity blackouts, which then cause direct impacts, such as accidents because of darkness. Third, the failure of one Critical Infrastructure can lead to the failure of another, when for example an electricity blackout has an impact on the water supply system, which might cause a water shortage for the general public. These so-called cascading effects can stretch on across several different infrastructures, if dependencies exist.

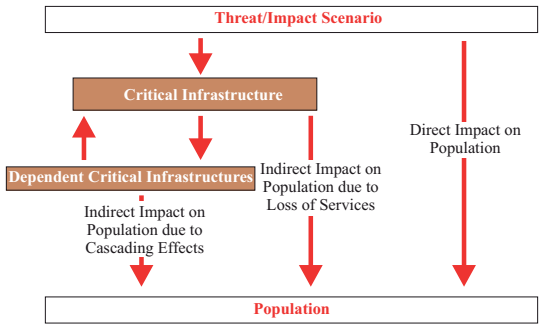

Fig. 1 Impacts of threats and Critical Infrastructure failure (BBK, 2013)

On the hazard and threat side, an all-hazard-approach is applied in Germany. For Critical Infrastructure Protection, this means that they are regarded under the influence of the entire spectrum of possible threats, which are classified into three types:

1. Natural events,
2. Technical failure/human error, and
3. Intentional acts such as terrorism, crime or war (see Fig. 2).

All of the different hazards and threats can cause failures of Critical Infrastructures. Which priority each of them is assigned, is object to the risk analysis process.

Natural Events	Technical Failure/ Human Error	Terrorism, Crime, War
Extreme Weather	System Failure	Terrorism
Forest/Heathland Fires	Negligence	Sabotage
Seismic Events	Accidents and Emergencies	Other Forms of Crime
Epidemics	Failures in Organization	Civil Wars and Wars
Cosmic Events		

Fig. 2 Threat Classification

Depending on the methodical approach, Critical Infrastructure failure can be considered as part of the (threat) scenario or as part of the effects that may be caused by the analyzed event. In the recent risk analyses on the national level in Germany, the expected Critical Infrastructure failures that go with a certain initial scenario (such as winter storm or flooding) are described in a qualitative way. Because of its outstanding importance for the supply of the population, the analysis of Critical Infrastructures failures and its consequences is one of the main tasks of the risk analyses. On the basis of this description, the expected damage to the population is described, using the four categories People (fatalities, injured, persons in need for public aid, persons missed), Environment (impairment of protected areas, impairment of water bodies, impairment of forests, impairment of agricultural land, impairment of livestock), Economy (impact on public administration, impact on private economy, impact on private households) and Immaterial (impact on public order and safety, political implications, psychological implications, damage of cultural assets), as can be seen in the respective reports (Deutscher Bundestag 2013a and 2013b). This way of treating Critical Infrastructures has the advantage that the assumed infrastructure damages and resulting disruptions of services are considered as input parameter for the impact assessment. Additionally, it makes clear that the disruption of their services is not only harmful in itself, but especially in its consequences for the population.

Results

Legal and Strategic Framework

The framework for Critical Infrastructure Protection in Germany is set by a number of documents with different character. The legal mandate for Civil Protection on the national level

is given by the Civil Protection and Disaster Assistance Act (ZSKG), which was passed in 2009. It defines the tasks of the Federal Office of Civil Protection and Disaster Assistance (BBK) within the German Civil Protection system. This system is strongly organized along the subsidiarity principle, giving a high level of competencies to the local and regional level (the Länder/federal states). §17 of the ZSKG entitles the Federal Office of Civil Protection and Disaster Assistance to collect and use data on Critical Infrastructures, and in §18 (2), it is stated that the federal government supports the Länder in the protection of Critical Infrastructures. The Federal Office of Civil Protection and Disaster Assistance is an authority within the remit of the Federal Ministry of the Interior.

The Civil Protection and Disaster Assistance Act specifies and gives legal authority to a document from 2002, the New Strategy for Civil Protection. It states that tasks in Civil Protection often require joint efforts of the national and the regional level and describes the way this could be done. It is important to note a specialty of the German Civil Protection system in this context, which is not shared by many other countries. The English term Civil Protection translates into two German words with different meanings: 1) *Zivilschutz*, meaning the protection of the citizens with non-military measures in cases of tension or defense and 2) *Katastrophenschutz*, meaning the protection of the citizens with non-military measures in cases of accidents or natural catastrophes. Only the first task is assigned to the national level, whereas the second task is to be performed by the Länder level. This distinction is founded in §§70 and 73 of the German Basic Constitutional Law. Since many civil protection measures can be of help in both cases, however, a cooperation between the two levels makes sense in many cases, as is specified in the ZSKG. As stated above, Critical Infrastructure Protection is one of the cases in which cooperation makes sense.

What else is necessary for successful Critical Infrastructure Protection is written down in the National Strategy for Critical Infrastructure Protection (German Federal Ministry of the Interior, 2009). It is the result of consultations among the different ministries on the federal government level. The most important statement is the commitment to a cooperative approach that includes government authorities, relief and emergency response organizations, private operators and their associations, the science and research community, the security industry, international and supranational institutions as well as the general public. While a trustful cooperation, coordination and information among the partners is the primary goal, the opportunity for legislation of course persists and may be used, if other measures do not succeed.

This set of documents is further supplemented by the Cyber Security Strategy for Germany from 2011, which has a focus on IT infrastructures (German Federal Ministry of the Interior, 2011). Regarding Critical Infrastructures in general, a paper on Protection Concepts for Critical Infrastructures (BBK, 2013) describes the different methods that are applied to enhance the protection level. These are analyses, studies and research projects, recommendations, guidelines and minimum standards, exercises, information exchange, discussion groups and work groups, consultancy and qualification and evaluation.

Cooperation of Stakeholders

The three main stakeholder groups are the public administration, the utility providers/operators and the population/general public. What each of them can do in order to enhance Critical Infrastructure Protection and how they can cooperate in this task, will be described in the following section.

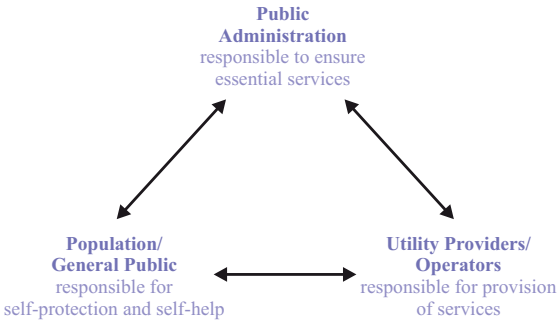

Fig. 3 Main stakeholder groups in Critical Infrastructure Protection

Each of the three main groups has different responsibilities within Civil Protection (see Fig. 3). The Public Administration has the responsibility to guarantee for their citizens' safety and security. This is expressed in the German Basic Constitutional Law as the right to life and physical integrity. While the state does not need to provide all the necessary goods and services, it has to enable third parties - the companies - to do so. In fields, in which the state does not take on the tasks itself, like it does in providing administration and rescue services, it sets the laws and the framework for the necessary services.

The utility providers have the responsibility to provide these services. For them, the goal of a safe provision of services is closely connected to their

own objectives. In providing services, they make profit, follow legal regulations, and take care of a good company image. Some even have a business continuity management in place, which serves the exact goal of keeping their processes running and the services available for their customers. Discrepancies to civil protection objectives arise, however, when additional protection measures seem too costly to justify them from an economic perspective. Here, the link between public administration and providers becomes important.

One solution of how a risk management can take place successfully between these two stakeholder groups is shown in Fig. 4. It shows different elements of risk management and assigns the main responsibility to one or both of them. The answer of the question "Who does it?" is of course derived from reflections on "Who can do what best?".

Threat scenarios, it is quite clear, are not the expertise of the operators. The public authorities have to provide them - be it according to probability/ plausibility, expected dimension of loss or political priorities. To shape them, the expertise of different authorities can be integrated, for example of the German Weather Service or the Federal Criminal Police Office. Also, the government has to provide the protective goals and clarify to which degree assets should be protected. In general, the provision of services becomes more expensive as the protection level is raised. Therefore, the target level needs to be given by the state authorities and not by companies whose principal interest lies in cost efficiency. The analysis of criticality, that is how meaningful a process or an asset is regarding the consequences of its failure, is a joint task. From a government level, the most important infrastructure services and infrastructures should be identified. Within the compound, operators identify their critical services and assets. The next question is how the given scenario can influence the critical assets, i. e. the analysis of vulnerability. This can be analyzed best from within the organization and is therefore the task of the operators. The protective measures, too, are within their responsibility. The operators have much more detailed knowledge of their internal processes and therefore it is in their responsibility to find the means to make their assets less vulnerable. The implementation and evaluation of the measures again is a joint task.

Cooperations like this between public authorities and utility providers can be put forward in different degrees of compulsion. They can be modes of operation in work groups, but it is also possible to give them a legal character. The focus of the German Critical Infrastructure Protection Strategy is cooperation. At present, there are great dynamics in the area of information security. Initiated by the Federal Office for Information Security, like the BBK within in the remit of the Ministry of the Interior, a platform has been established for the dialogue among Critical Infrastructure operators and government authorities. The sectoral and thematic work groups of the so-called UP KRITIS provide the opportunity to exchange information and discuss safety and security solutions. Also in the sector of information and telecommunication, a legal initiative is being discussed in Germany. A proposition for an IT Security Law is being discussed, which would make it mandatory for Critical Infrastructure operators to report cyber attacks or technical failures.

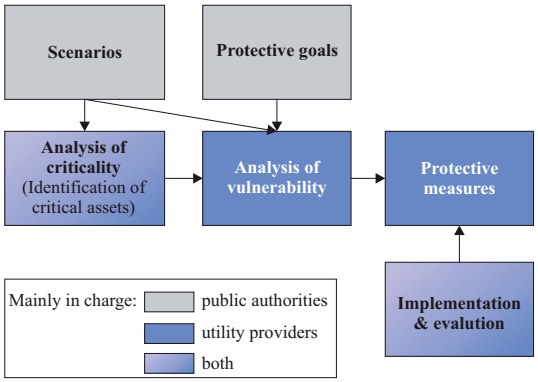

Fig. 4 Blue-print for responsibilities of public authorities and utility providers in Critical Infrastructure Protection (BBK)

The most important stakeholder is, in a way, the population. They are the target of Civil Protection, the reason why infrastructures are run and why measures for their protection are taken at all. In addition to being the reason for the other stakeholders' actions, they bear a great responsibility for self-help. This already follows the fact that in great events, the most immediate, most direct measures are the ones taken by individual persons themselves. They can help to solve emergency situations, for example by keeping sufficient food and water provisions for their own needs or by rendering first aid to injured co-citizens. In the first phases of catastrophes, they are often the only ones in place, and they can often help more effectively than any organization can. They are most familiar with the adjacencies and in their multitude, they provide a great potential for creative solutions.

In times of social media, it is more important than ever to note that the population is so much more than the object to be protected, but also the active helper that can make negative effects take a much milder form and that can also be directed in its actions to

provide aid where it is needed. How to improve this integration of self-organized help from the population and the traditional organizations is one of the great challenges of modern Civil Protection.

Critical Infrastructure Protection along the Risk and Crisis Management Cycle

On the one hand, public authorities and the BBK in particular, play an active role in Critical Infrastructure Protection, e. g. by presenting threat scenarios that infrastructures are to be protected against. Apart from this role as one of the players, there is also support for other stakeholders to be provided, according to the legal and strategical framework. The BBK and the Federal Ministry of the Interior therefore publish guidelines and support other players in manifold ways. In the following, examples of this will be given along the lines of the risk and crisis management cycle, which is the baseline for Civil Protection (see Fig. 5). The performance and integration of prevention, preparedness, incident response and recovery make up for a successful risk and crisis management.

Fig. 5 Risk and Crisis Management Cycle

The work on Critical Infrastructures in the German Federal Ministry of the Interior and the Federal Office of Civil Protection and Disaster Assistance takes place in all four phases, but has a focus in the prevention and preparedness phase. Examples of this are a guideline for enterprises as well as for public authorities for their internal risk management (BMI, 2011) and technical guidelines for risk and crisis management for electricity grid operators (VDE-FNN, 2011, and VDE-FNN, 2012). The latter was developed under the lead of a professional association, involving different operators as well as the BBK. An example for enhancing preparedness on the individual level is a guideline for the population that addresses different kinds of catastrophes and gives advice on how to prepare for them (BBK, 2009). To prepare the decision takers on the national and regional level, the LÜKEX cross-Länder exercise in national crisis management is carried out every two years, jointly conducted by the Federation and the Länder. For the case of electricity blackouts, a very detailed handbook gives advice on the prevention and preparedness phase to public administration as well as Critical Infrastructure operators.

In the response phase, the BBK gives support to the public authorities with the German Joint Information and Situation Centre (GMLZ) and to the population with the Coordination Office Aftercare, Support for Victims and their Relatives (NOAH), to name just two of its services. For the recovery phase and the follow-up procedures after an event, the Technical Information System (FIS) within the BBK provides useful information to learn for the future from past events. It is the largest specialized library in Germany on the area of civil and disaster protection.

Conclusion

With surveys, analyses, round-tables, expert networks, research and training courses, one goal is to be achieved: to make the failure of Critical Infrastructure less likely and - in cases it does happen anyway - less devastating. This cannot be done by one stakeholder alone, which is why the exchange and cooperation of all the stakeholders is so important, across organizations and also across national borders.

Acknowledgments

This article was written with contributions from Alexander Esser, Susanne Krings, Peter Lauwe, Susanne Lenz and Kathrin Stolzenburg (all German Federal Office of Civil Protection and Disaster Assistance (BBK), Bonn, Germany).

References

BBK (2013). *Schutzkonzepte Kritischer Infrastrukturen im Bevölkerungsschutz. Ziele, Zielgruppen, Bestandteile und Umsetzung im BBK* (Wissenschaftsforum, 11) [online, cit. 2014-10-29]. Available at: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Wissenschaftsforum/Bd_11_Schutzkonzepte_KRITIS.pdf?__blob=publicationFile.

BBK (2009). *How to be Prepared for an Emergency. Prevention and Self-Help in Emergency Situations* [online]. 11th edit. Bonn, Germany [cit. 2014-10-28]. Available at: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Broschueren_Flyer/Fremdsprachliche_Broschueren_fdNv/Broschuere_fdNv_englisch.pdf?__blob=publicationFile.

BBK, IM BW, KIT (2010). *Krisenhandbuch Stromausfall Baden-Württemberg. Handbuch mit Planungshilfen*. Heidelberg, 2010.

BMI (2011). *Schutz Kritischer Infrastrukturen - Risiko - und Krisenmanagement. Leitfaden für Unternehmen und Behörden* [online, cit. 2014-10-29]. Available at: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf?__blob=publicationFile.

DEUTSCHER BUNDESTAG (2013a). *Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2013* (Drucksache 18/208) [online, cit. 2014-10-29]. Available at: http://dip21.bundestag.de/dip21/btd/18/002/1800208.pdf.

DEUTSCHER BUNDESTAG (2013b). *Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2012* [online]. (Drucksache 17/12051) [cit. 2014-10-29]. Available at: http://dip21.bundestag.de/dip21/btd/17/120/1712051.pdf.

GERMAN FEDERAL MINISTRY OF THE INTERIOR (2011). *Cyber Security Strategy for Germany* [online]. Berlin, Germany, 2011 [cit. 2014-10-29]. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.

GERMAN FEDERAL MINISTRY OF THE INTERIOR (2009). *National Strategy for Critical Infrastructure Protection (CIP Strategy)* [online]. Berlin, Germany, 2009 [cit. 2014-10-28]. Available at: http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf.

VDE-FNN (2012). *S 1001 - Sicherheit in der Stromversorgung. Hinweise für das Risikomanagement des Netzbetreibers*. Berlin, 2012.

VDE-FNN (2011). *S 1002 - Sicherheit in der Stromversorgung. Hinweise für das Krisenmanagement des Netzbetreibers*. Berlin, 2011.