Knowledge management for the protection of critical infrastructures

N. Gronau, T. Röchert-Voigt & N. Proske
Chair of Business Information Systems and Electronic Government, University of Potsdam, Germany

Abstract

The presented ongoing research project focuses on the challenges concerning the protection of critical infrastructures. Since critical infrastructures become more and more cross-linked a single breakdown can cause serious cascading effects on other infrastructures. Interdependencies of critical infrastructures are boundary-spanning and therefore public authorities, operating companies and other stakeholders (e.g. German Federal Agency for technical relief, Red Cross) as well as stakeholders of neighbouring states must have access to a solution which enables the urgently needed cooperation of all parties involved. The aim of the project is to develop an online platform to facilitate knowledge exchange among stakeholders, an online tool to analyse the interdependencies and to design a sustainable and effective knowledge management. This platform will allow registered members to find and make use of the information about the stakeholders and their competencies concerning the protection of critical infrastructures.
Keywords: EUKRITIS, online-platform, information exchange, knowledge-map, interdependency, social software, Web 2.0, knowledge management, networking, cross-linking.

1 Introduction – why knowledge management?

Providing security is without any doubt one of the main functions of a state. For philosophers such as Thomas Hobbes is the ability of guaranteeing security constitutive for a state. Without this ability, states are futile. In order to provide security states use specific instruments that, according to the German philosopher Jürgen Habermas, also represent a certain period of state regulation


WIT Transactions on the Built Environment, Vol 117, © 2011 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE110021

[1]. Hobbes' central figure, a war of all against all, is predominantly focused on providing personal security as well as ensuring the compliance of contracts. However, in a modern society, the regulation of risks, such as technological or environmental risks, can be regarded as the latest challenge for security grant efforts.

Habermas periodisation of developments in the guarantee of security by the state is divided into three periods. Each of these periods is characterized by a certain degree of state activity and scope of regulations but also by the positive assumption of always being able to ensure security.

Further developments and consequently the extent of the state guarantee of security are both results of risks that are caused by science and technology as well as responses to changing social conditions [1]. There is also a greater willingness of society to take risks by transforming threats, which they once regarded with fatalism, to risks [2] and thus make them available for independent decisions [3]. State's instruments have, in order to deal with it, shifted, too. Established instruments such as legislation and resource allocation – authority and money – are about to reach their limits. The legal state and hence its specific instrument, threat of punishment, would fail if causalities could not be assigned for each case anymore or if damages were results of actions that are principally desirable.

However, monetary compensation – the social state's specific instrument – will be overstrained if impacts of damages exceed any capabilities of compensation. In particular, industrial and scientific/technical-projects are already off any private sector capabilities, they are uninsurable risks (e.g. nuclear power plants or chemical plants) [4]. As a result, the preventive state has emerged [1]. Instead of dealing with individual threats, hazardous situation are regarded on a collective level, as the preventive state emerged. Hazards must be identified in advance in order to prevent their occurrence. A specific instrument now is knowledge. However, one resource is not replaced by another. Rather the manner of using a resource changes. Knowledge is not the authority's specific and exclusive instrument of superiority anymore as Max Weber once described [5]. Also due to global meta-trends like globalisation, liberalisation and privatisation an integrative and multidisciplinary approach between security authorities and the industry as operators of critical infrastructure, is needed. Each player involved - whether the operators of critical infrastructure itself or authorities - has to provide immediate response and protection plans due to legal regulations. These plans include, for instance, the organizational structure and operational plans in a critical situation. In order to assure an effective and efficient crisis management, it is crucial to coordinate protection plans within a protection system Involved actors need to be able to identify the existing competencies and capabilities of each other within the protection system.

To analyse the interaction of public authorities, business and science in the process of protection of critical infrastructure and to develop concepts for a sustainable und effective knowledge management is the aim of a research project, funded by the European Commission, Directorate-General Humanitarian Aid – ECHO. Associated partner are the Ministry of Interior of the Federal State

of Brandenburg, the University of Potsdam, the local distribution network operator Netzgesellschaft Berlin-Brandenburg mbH &Co.KG (NBB) and the fire department headquarters of the voivodeship West Pomerania (Poland).

2 Objects of research, motivation and benefits

Since the interdependencies of critical infrastructures are boundary-spanning, public authorities, operating companies, aid organisations, disaster relief organisations (e.g. Red Cross, THW) as well as stakeholders of neighbouring states must have access to an integrated solution that enables immediate cooperation of all parties involved. Successful protection of critical infrastructures means functioning operators and protected societies that are boundary-spanning. Boundaries can be understood as administrative districts or regional districts. Keeping this in mind, the project focuses on the cooperation of the stakeholders as well as a sustainable and an effective knowledge management. Therefore we develop an online portal (EUKRITIS-Portal) to establish a closer connection and facilitate a network of stakeholders. Furthermore we develop an interactive knowledge-map and a tool to analyse the interdependencies of critical infrastructures. The EUKRITIS-Portal is not intended to substitute the already established ways of communication. Its aim is rather to supplement these ways by providing more elaborate instruments.

The benefits for the stakeholders are the network of operators of critical infrastructures, public authorities, providers in the security field, science and other private organisations. Moreover, the functional exchange of information about best practises and tools will be encouraged. The tool to analyse interdependencies will record the dependency types to enable the coordination of arrangements before any disaster happens, to minimize cascade effects particularly. An institutional contact of public authorities in the field of protection of critical infrastructures will also be defined.

3 Impacts on exchange of knowledge

What is actually meant by the knowledge necessary to accumulate and exchange? And what is the problem? In a survey among actors in the field of critical infrastructures in the German state Brandenburg, both the most inhibiting and facilitating factors of knowledge exchange have been collected and identified. A survey in the voivodeship West Pomerania, Poland, which was conducted at the same time, has shown similar results, approving that the factors identified are by no means limited to a certain state or country, though there are differences due to cultural or political traditions.

According to the survey, the exchange of information is highly time-consuming. Furthermore there is a lack of clarity in contacts and especially a lack of common understanding in fundamental terms. Each stakeholder has its own terminology, partly deriving from specific but different legal regulations. Another factor inhibiting information exchange stakeholders have named is the varying levels of knowledge in the field of disaster management. The latter is

somehow to expect, given the diverse scopes and subjects of the actors involved. It is obvious that research institutions, fire departments, authorities or businesses focus on specific but not automatically converging fields when dealing with disaster management. But there are several obstacles on the way towards a collaborative approach in disaster prevention. One has to keep in mind that business continuity refers to business-critical domains. Thus, the sharing of elaborate information would be possible, when only in case of a highly confidential environment. It was not surprising that security concerns were identified as a major inhibiting factor for the exchange of knowledge. Certain information needed to be exchanged in order to generate benefits from collaboration and organisation can unfold a potential for damage at the same time. Another crucial factor is a competitive environment, for businesses in particular. An exchange of delicate information such as security risks or the overall expense for security means seems quite unlikely if there is no crucial benefit. But there also factors facilitating the exchange of knowledge. Respondents emphasised the importance of personal contacts and existing mutual trust. They often know their counterparts in other businesses or authorities personally, due to joint projects, conferences or joint exercises. The challenge is to achieve a similar level of reliance and trust by transparency and a sophisticated role-based access control. Further facilitating factors identified are certain duties to supply information as well as expected benefits, which can be named as the main impact factor to encourage participation. Only when there is a surplus value, organisations are likely to participate. A collaborative approach will always fail if there is no participation.

4 Cross-linking and networking via the EUKRITIS-portal

Web portals are popular in the World Wide Web (WWW). The main entrance concept via a web portal has proved itself useful for access to the variety of information in the WWW by allowing the access to structured information about special topics. Furthermore, a web portal allows many people for cross-linking and networking. Thus web portals are qualified for the knowledge-management of enterprises in general, but also appropriate in the more heterogeneous field of disaster prevention. Web portals in general are part of the well-known term Web 2.0 and sometimes of the term Social Software, too. In fact there is no general definition of both terms at all. The term Web 2.0 comprehends several extremely different things like specific techniques, standards and programmes or computer applications, e.g. AJAX as a technique, RSS as a family of standards or wikis and blogs as computer applications. Social software applications are for example wikis, blogs and forums. Sometimes the term Web 2.0 and term social software are even used synonymously. But social software unlike Web 2.0 does not mean any specific techniques, standards or programmes [6, 7] and therefore the terms should not be used synonymously. Both terms due to integrate users. Specific techniques, standards or programs assigned to Web 2.0 are the basic requirement of social software applications. In fact, social software applications include socio-technical and web-based computer applications that serve the

communication, coordination and collaboration of people within the social context of networking [9] and therefore are a specific part of Web 2.0. These applications focus on three interaction modes of user integration (three C´s): communication, coordination and collaboration. These modes are based logically on each other [8, 7]. Communication means the information exchange and is necessary for the coordination of activities. With regard to the achievement of objectives collaboration is essential. Therefore collaboration without coordination and communication is not possible, neither is information exchange without social networking previously. According to Birn, Müller and Gronau, these interaction modes can be assigned to the following social software applications [10–12]:

Based on these interaction modes, the social software applications are varied, but have different main characteristics as presented in figure 1, in particular:

- Synchronous or asynchronous communication via instant messaging, chat, blog or forum
- Separating contents or information sources, e.g. CiteULike, Delicious
- Building and maintaining contacts, e.g. Facebook, Xing, different VZs
- Common building of documents for instance via wiki
- Participation via online consultations or local budget platforms

The EUKRITIS web platform is classified as Web 2.0 element. The integrated applications are classified as social software.

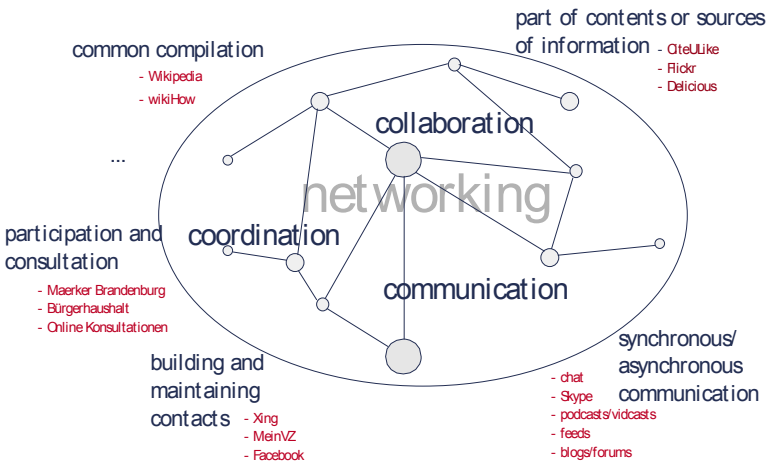

Figure 1: Social software (according to [7, 8, 12]).

The platform will be established in the field of critical infrastructures. Mainly the platform should be used for communication and information exchange prior to a crisis. Since stakeholders are expected to be constantly available especially in times of crisis, this portal was not designed to be used as an instrument in dealing with a crisis situation although this is not impossible.

The platform integrates several applications that were derived from requirements identified through a survey and evolved in two workshop sessions. The aim is not to substitute existing communication channels but to complement them. The following Social Software applications were prioritised by the MuSCoW-prioritisation and focused on the aims of the project. First of all there is a geo-based knowledge map as reference finder that includes the organisation profile, contact person and direct contact possibility (must-have). The knowledge map is developed according to the terms critical infrastructures and searching in this field. Furthermore there must be a wiki to exchange information, documents and resources and refine them by discussing and reviewing. A wiki must also facilitate the exchange of best-practices. To add all best-practises the same way a structure is specified. Also there is a tool to analyse the interdependencies (must-have). This will be realised by a form-based query included evaluation and report functions. A self-made ad hoc Wiki will be desirable (should-have) in order to design concepts and standards for workflows or operation charts conjointly. These concepts and standard should become engaging by a voting option of all registered platform members.

Focused on the possibility to get in contact with other stakeholders more networking applications are required to build up working groups by registered members in special fields, e.g. risk communication, standardization of terms for common understanding. According to the applications and the security requirements (data protection and security) the concept of roles and legal authorisation is developed. Furthermore a market place for completed, ongoing and future projects will be offered to the registered members to find experience and partners. A market place for companies in the field of security to offer as well as search products and services will also be part of the platform. At least there should be applications for Instant Messaging, RSS-Feeds for information updates, a sampler of links like Delicious and a calendar of events.

5 Knowledge-map

The major element of the EUKRITIS platform is the knowledge-map. This is a geo-based map and reference-finder similar to Yellow Pages. The difference on the one hand is the visualisation in the field of critical infrastructure by a GIS system. On the other hand not only the stakeholders are located but also their field of knowledge. The field of knowledge is first classified into sectors and subsectors. First of all we focussed on the energy sector with all its subsectors like electricity, gas, oil, water, solar, wind and mining industry. Moreover, there is a hazard based approach to specify fields of knowledge based on three categories of each subsector: forces of nature, technical or humane breakdowns and terrorism. Therefore we found out many disasters in this categories and determined knowledge fields for instance business continuity management, high-voltage installation, radioactive waste management or security of supply for example in the sector of energy, subsector electricity. Those fields are refined as a list. Stakeholders who are registered will be able to choose their sector- and subsector-specified field of knowledge via a drop-down menu. Stakeholders

mean the organisations and their employees themselves. Each organisation will be able to choose its knowledge fields in general as well as each employee of the organisation who is allowed to.

The included organisation or people profile, the contact person and a direct contact as well as the knowledge field will be offered to registered members only. The knowledge-map is therefore a composition of know-how-existence and expert-directory. The search results are processed graphically and shown visualised within the scope of a map.

Not registered and authorised people can get visualised general information about the stakeholder-organisation only as found in the WWW, telephone directory or Yellow Pages like the general organisation profile, location and general contact. The main benefit for registered and authorised members is finding experts and be found as expert for special questions in sectors, subsectors and lines of business in the field of critical infrastructures. Therefore they are able to cooperate and improve their own protection system with focus on the total system the own organisation is part of. The knowledge-map is just implementing.

6 Analysis of interdependencies

It has become consensus that each part of public and private life is highly affected by complex and cross-linked (critical) infrastructures. Damages and breakdowns cause high impacts on both the supply of necessary goods and services and on the public security. It has to be considered that critical infrastructures do not end at frontiers but are cross-linked regarding regional and international dependencies. Within an ideal network each organisation generates the other organisation's input, their factors of production. Naturally, each actor is supposed to be aware of the factors of production they need. For instance one assumes that employees are able to come to work every morning. In case of malfunctioning of a vital junction, loss of production due to missing manpower would not be an exotic scenario. To identify such undesigned interdependencies among critical infrastructures is a second central pillar of the portal, represented by a web-based method for a largely self organised interdependence analysis. As a result possible cascade effects will be identified and can be eased. The approach shall provide key figures specific to individual outputs.

Operators of critical infrastructures will have to provide data which is specific to their organisation and their geographical environment; the sector and the geographic location determine the further data collection. The analysis will include geographic as well as functional interdependencies. For instance, it makes a difference whether there is just one appropriate road to a factory or options to substitute. In a second step proposed content will be processed and completed. Based upon personal data as well as data from organisations of the same sector a comparative analysis of the varying interdependencies in a normal situation and in a crisis situation will be conducted. Individual dependencies will be displayed afterwards. But also an analysis for certain cases of damage, based

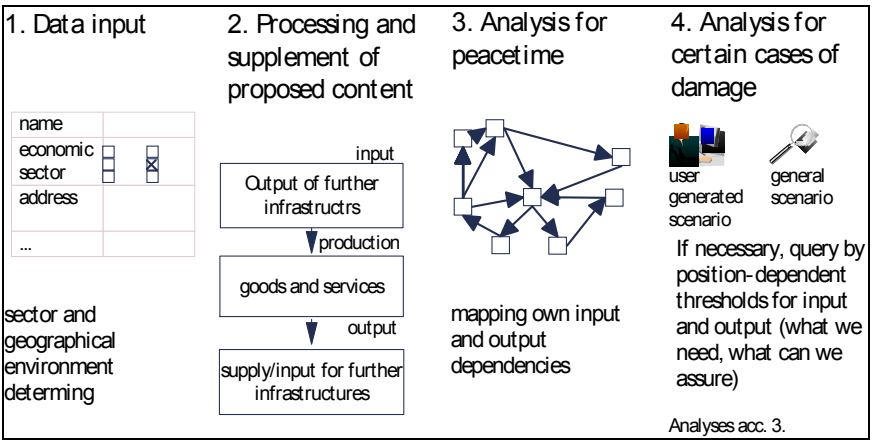

Figure 2: Process from a user-perspective.

on either a user generated scenarios or general scenarios is intended to be integrated.

7 Conclusion

The project is facing serious challenges to sustainability. Precisely because it is conceived as extension of established communication channels, it has to prove its beneficial character. As mentioned above, each collaborative project depends on user participation – and is doomed to failure if user generated content is missing. In order to ease this vicious circle the platform will be equipped with the features described above. In particular the knowledge map and interdependence analysis generate a first surplus value, addressing some of the obstacles our data collection has identified. The former will be provided with initial content. Actors involved in protection of critical infrastructure in German state Brandenburg will be enlisted in order to demonstrate the platforms capability.

On its way to service a testing phase is held in summer focussing in particular on usability and user acceptance. The knowledge-map was already presented and discussed on the computer expo CeBIT 2011 in Germany. Based on numerous positive feedbacks on preceding research project EUKRITIS I, focussing the change capability of protection systems [13], community guidelines are planned to be created, in order to ensure the further use after the project has finished.

The exchange of knowledge among relevant actors will be facilitated, hence the protection of critical infrastructures as well the supply of the population will be ensured. At the end of the project, the main challenge will be to motivate and convince relevant stakeholders of using this additional channel of communication, after all it firstly means additional workload. A sophisticated role-based access control will counteract worries about reliability and data protection.

References

[1] Habermas, J. (1992): Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaates, Frankfurt am Main: Suhrkamp.

[2] Morandi, P. (2004): Der Wille zum Risiko in modernen Gesellschaften, in: Edeling, T.; Jann, W.; Wagner, D. (Ed.): Wissensmanagement in Politik und Verwaltung, Wiesbaden: VS Verlag., pp. 37–56.

[3] Luhmann, N. (1991): Soziologie des Risikos, New York, de Gruyter.

[4] Beck, U. (2007): Weltrisikogesellschaft, Frankfurt am Main: Suhrkamp.

[5] Weber, M. (1972): Wirtschaft und Gesellschaft, Grundriss der verstehenden Soziologie, Tübingen: Mohr.

[6] Hippner, H. (2006): Bedeutung, Anwendungen und Einsatzpotentiale von Social Software. In: Hildebrand, K.; Hofmann, J. (Ed.): Social Software. HMD - Praxis der Wirtschaftsinformatik, Vol. 252, Heidelberg: dpunkt.verlag, pp. 6-16.

[7] Riemer, K. (2009): eCollaboration: Systeme, Anwendungen, aktuelle Entwicklungen. In: Riemer, K.; Strahringer, S (ed.): eCollaboration. HMD – Praxis der Wirtschaftsinformatik, Vol. 267, Heidelberg: dpunkt verlag, pp. 7-17

[8] Teufel, S. et al. (1995): Computerunterstützung für die Gruppenarbeit, Bonn: Oldenbourg.

[9] Röchert-Voigt, T. (2010): Einsatz von Social Software im Beteiligungs-verfahren zur Rechtsetzung, in: eGovernment Kompendium 2011 – IT Refe-renzbuch für den Öffentlichen Sektor, Augsburg, pp. 66-68

[10] Birn, L.; Müller, C. (2006): Kollaboratives Dokumentieren mit Sozialer Software, In: ERP-Management - Zeitschrift für unternehmensweite Anwen-dungssysteme, Vol. 2, pp. 36 - 39.

[11] Müller, C.; Gronau, N. (2007): Bildung von sozialen Netzwerken in Anwendungen der Social Software. In: Müller, C.; Gronau, N.: Analyse sozialer Netzwerke und Social Software - Grundlagen und Anwendungs-beispiele, Berlin: Gito-Verlag: pp. 1-24.

[12] Gronau, N. (2009): Soziale Software. In: Kurbel, K. et al. (Ed.): Enzyklopädie der Wirtschaftsinformatik – Online-Lexikon. München: Oldenbourg, http://www.enzyklopaedie-der-wirtschaftsinformatik.de/ (22.01.2011)

[13] Gronau, N.; Sielaff, S.; Weber, E.; Röchert-Voigt, T.; Stein, M. (2009): Change capability of protection systems. In Duncan, K., & Brebbia, C. A. (Ed.), Disaster Management and Human Health Risk: Reducing Risk, Improving Outcomes (Wit Transactions on the Built Environment). WIT Press, pp. 87-95.